

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-100116

(P2002-100116A)

(43) 公開日 平成14年4月5日(2002.4.5)

(51) Int.Cl. 識別記号

G 1 1 B 20/10

G 1 0 L 11/00

H 0 4 L 9/32

F I

G 1 1 B 20/10

G 1 0 L 9/00

H 0 4 L 9/00

テ-マコト* (参考)

H 5 D 0 4 4

E 5 J 1 0 4

6 7 3 A

6 7 3 E

6 7 3 D

審査請求 未請求 請求項の数149 O L (全 25 頁)

(21) 出願番号 特願2000-260467(P2000-260467)

(22) 出願日 平成12年8月30日(2000.8.30)

(31) 優先権主張番号 特願2000-216388(P2000-216388)

(32) 優先日 平成12年7月17日(2000.7.17)

(33) 優先権主張国 日本(J P)

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72) 発明者 猪口 達也

東京都品川区北品川6丁目7番35号 ソニ
ー株式会社内

(72) 発明者 佐古 曜一郎

東京都品川区北品川6丁目7番35号 ソニ
ー株式会社内

(74) 代理人 100091546

弁理士 佐藤 正美

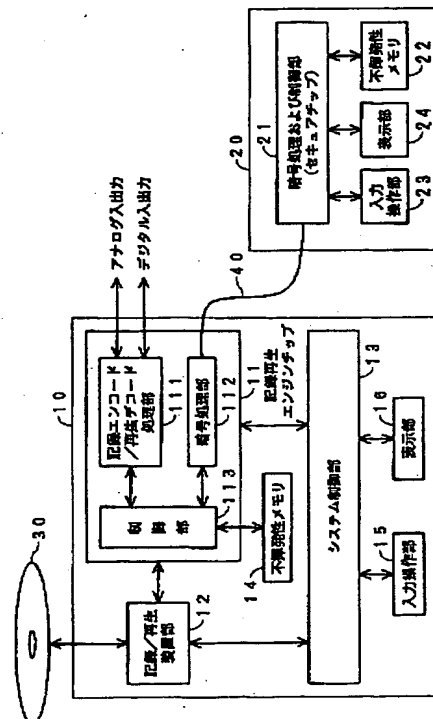
最終頁に続く

(54) 【発明の名称】 データ記録再生方法および装置、データ記録装置および方法、データ再生装置および方法並びに記録媒体

(57) 【要約】

【課題】 個人使用の範囲での複製は自由にし、かつ、業とした不正な複製を有効に防止する。

【解決手段】 所定の記録データの記録時には、ユーザIDモジュール20を記録再生装置10に接続し、使用者を特定するための使用者識別情報をユーザIDモジュールから取得して、記録データと共に、記録媒体30に記録する。所定の記録データの再生時には、記録媒体30からの情報から検出された使用者識別情報と、不揮発性メモリ14から読み出した使用者識別情報とが一致したときは、記録情報の再生を許可する。



【特許請求の範囲】

【請求項 1】記録データの記録時には、使用者を特定するための使用者識別情報を、前記記録データと共に、記録媒体に記録し、

前記記録データの再生時には、前記記録媒体からの情報から検出された前記使用者識別情報と、前記記録媒体以外から取得した前記使用者識別情報とが一致したときは、前記記録データの再生を許可することを特徴とするデータ記録再生方法。

【請求項 2】請求項 1 に記載のデータ記録再生方法において、
前記使用者識別情報が予め記憶された不揮発性メモリを設け、前記再生時には前記不揮発性メモリから読み出した前記使用者識別情報を、前記記録媒体以外から取得した前記使用者識別情報とすることを特徴とするデータ記録再生方法。

【請求項 3】請求項 1 に記載のデータ記録再生方法において、
前記記録データは、暗号化されており、前記再生時において、前記記録媒体からの情報から検出された前記使用者識別情報と、前記記録媒体以外から取得した前記使用者識別情報とが一致したときに、前記暗号化が解除されることを特徴とするデータ記録再生方法。

【請求項 4】請求項 3 に記載のデータ記録再生方法において、
前記記録データの暗号化は、前記使用者識別情報に関連付けられていることを特徴とするデータ記録再生方法。

【請求項 5】請求項 1 に記載のデータ記録再生方法において、

前記記録データの記録時には、記録装置とは別体の使用者識別情報提供装置から、前記使用者識別情報を取得するようにすることを特徴とするデータ記録再生方法。

【請求項 6】請求項 5 に記載のデータ記録再生方法において、

前記使用者識別情報提供装置が前記記録装置に接続されていないときには、前記記録データの記録を不可とすることを特徴とするデータ記録再生方法。

【請求項 7】請求項 5 に記載のデータ記録再生方法において、

前記使用者識別情報が予め記憶された不揮発性メモリを設け、前記不揮発性メモリから読み出した前記使用者識別情報を、前記記録媒体以外から取得した前記使用者識別情報とすることを特徴とするデータ記録再生方法。

【請求項 8】請求項 5 に記載のデータ記録再生方法において、

前記使用者識別情報提供装置からの前記使用者識別情報は、暗号化して、前記記録装置に供給するようにすることを特徴とするデータ記録再生方法。

【請求項 9】請求項 5 に記載のデータ記録再生方法において、

前記使用者識別情報提供装置からの前記使用者識別情報は、予め前記使用者識別情報提供装置に格納された当該装置ごとに固有の情報であることを特徴とするデータ記録再生方法。

【請求項 10】請求項 1 に記載のデータ記録再生方法において、

前記使用者識別情報は、指紋、声紋、脈などの生体情報であることを特徴とするデータ記録再生方法。

【請求項 11】請求項 1 に記載のデータ記録再生方法において、

前記記録データと共に前記記録媒体に記録する前記使用者識別情報は、前記記録データに埋め込むことを特徴とするデータ記録再生方法。

【請求項 12】使用者を特定するための使用者識別情報を取得するための第 1 の使用者識別情報取得工程と、

前記第 1 の使用者識別情報取得工程で取得した前記使用者識別情報を、記録データと共に、記録媒体に記録する記録処理工程と、

前記使用者識別情報を取得するための第 2 の使用者識別情報取得工程と、

前記記録媒体からの情報から前記使用者識別情報を検出する使用者識別情報検出工程と、

前記使用者識別情報検出工程で検出された前記使用者識別情報と、前記第 2 の使用者識別情報取得工程で取得した使用者識別情報とが一致するか否かを判定する判定工程と、

前記判定工程において、前記使用者識別情報が一致したと判定されたときに、前記記録媒体に記録されている前記記録データの再生を許可して再生を実行するようにする再生処理工程と、

を備えるデータ記録再生方法。

【請求項 13】請求項 12 に記載のデータ記録再生方法において、

前記第 1 の使用者識別情報取得工程と、前記第 2 の使用者識別情報取得工程とでは、前記使用者識別情報が予め記憶された不揮発性メモリから、前記使用者識別情報を読み出すことを特徴とするデータ記録再生方法。

【請求項 14】請求項 12 に記載のデータ記録再生方法において、

前記第 1 の使用者識別情報取得工程と、前記第 2 の使用者識別情報取得工程とでは、記録ないし再生装置とは別体の使用者識別情報提供装置から、前記使用者識別情報を取得することを特徴とするデータ記録再生方法。

【請求項 15】請求項 12 に記載のデータ記録再生方法において、

前記第 1 の使用者識別情報取得工程では、記録ないし再生装置とは別体の使用者識別情報提供装置から、前記使用者識別情報を取得し、

前記第 2 の使用者識別情報取得工程では、前記使用者識別情報が予め記憶された不揮発性メモリから、前記使用

者識別情報を読み出すことを特徴とするデータ記録再生方法。

【請求項 16】請求項 12 に記載のデータ記録再生方法において、前記記録データは、暗号化されており、前記再生時において、前記記録媒体からの情報から検出された前記使用者識別情報と、前記第 2 の使用者識別情報取得工程で取得された前記使用者識別情報とが一致したときに、前記暗号化が解除されることを特徴とするデータ記録再生方法。

【請求項 17】請求項 12 に記載のデータ記録再生方法において、前記記録データの暗号化は、前記第 1 の使用者識別情報取得工程で取得された前記使用者識別情報に関連付けられていることを特徴とするデータ記録再生方法。

【請求項 18】請求項 12 に記載のデータ記録再生方法において、前記第 1 の使用者識別情報取得工程で、前記使用者識別情報が取得できないときには、前記記録データの記録を不可とすることを特徴とするデータ記録再生方法。

【請求項 19】請求項 14 または請求項 15 に記載のデータ記録再生方法において、前記使用者識別情報提供装置からの前記使用者識別情報は、暗号化されていることを特徴とするデータ記録再生方法。

【請求項 20】請求項 14 または請求項 15 に記載のデータ記録再生方法において、前記使用者識別情報提供装置からの前記使用者識別情報は、予め前記使用者識別情報提供装置に格納された当該装置ごとに固有の情報であることを特徴とするデータ記録再生方法。

【請求項 21】請求項 12 に記載のデータ記録再生方法において、前記使用者識別情報は、指紋、声紋、脈などの生体情報であることを特徴とするデータ記録再生方法。

【請求項 22】請求項 12 に記載のデータ記録再生方法において、前記記録データと共に前記記録媒体に記録する前記使用者識別情報は、前記記録データに埋め込むことを特徴とするデータ記録再生方法。

【請求項 23】記録データと共に、使用者を特定するための使用者識別情報を、記録媒体に記録する記録手段と、前記記録媒体からの情報から検出された前記使用者識別情報と、前記記録媒体以外から取得した前記使用者識別情報とが一致したときに、前記記録情報の再生を許可する制御手段と、を備えることを特徴とするデータ記録再生装置。

【請求項 24】請求項 23 に記載のデータ記録再生装置において、

10 再生時において、前記記録媒体からの情報から検出された前記使用者識別情報と、前記記録媒体以外から取得した前記使用者識別情報とが一致したときに、前記暗号化が解除されることを特徴とするデータ記録再生装置。

【請求項 25】請求項 23 に記載のデータ記録再生装置において、

前記記録データの暗号化は、前記使用者識別情報に関連付けられていることを特徴とするデータ記録再生装置。

【請求項 26】請求項 23 に記載のデータ記録再生装置において、

20 前記記録データの記録時には、記録再生装置とは別体の使用者識別情報提供装置から、前記使用者識別情報を取得するようにすることを特徴とするデータ記録再生装置。

【請求項 27】請求項 27 に記載のデータ記録再生装置において、前記使用者識別情報提供装置が前記記録装置に接続されていないときには、前記記録データの記録を不可とすることを特徴とするデータ記録再生装置。

【請求項 28】請求項 27 に記載のデータ記録再生装置において、前記使用者識別情報が予め記憶された不揮発性メモリを備え、

前記不揮発性メモリから読み出した前記使用者識別情報を、前記記録媒体以外から取得した前記使用者識別情報とすることを特徴とするデータ記録再生装置。

【請求項 29】請求項 27 に記載のデータ記録再生装置において、前記使用者識別情報提供装置からの前記使用者識別情報は、暗号化されていることを特徴とするデータ記録再生装置。

【請求項 30】請求項 27 に記載のデータ記録再生装置において、前記使用者識別情報提供装置からの前記使用者識別情報は、予め前記使用者識別情報提供装置に格納された当該装置ごとに固有の情報であることを特徴とするデータ記録再生装置。

【請求項 31】請求項 27 に記載のデータ記録再生装置において、前記使用者識別情報は、指紋、声紋、脈などの生体情報であることを特徴とするデータ記録再生装置。

【請求項 32】請求項 23 に記載のデータ記録再生装置において、前記使用者識別情報は、指紋、声紋、脈などの生体情報であることを特徴とするデータ記録再生装置。

【請求項 3 3】請求項 2 3 に記載のデータ記録再生装置において、

前記記録データと共に前記記録媒体に記録する前記使用者識別情報は、前記記録データに埋め込むことを特徴とするデータ記録再生装置。

【請求項 3 4】使用者を特定するための使用者識別情報を取得するための第 1 の使用者識別情報取得手段と、前記第 1 の使用者識別情報取得手段で取得した前記使用者識別情報を、記録データと共に、記録媒体に記録する記録処理手段と、

前記使用者識別情報を取得するための第 2 の使用者識別情報取得手段と、

前記記録媒体からの情報から検出した前記使用者識別情報と、前記第 2 の使用者識別情報取得手段から取得した使用者識別情報とが一致したときには、前記記録媒体に記録されている前記記録データの再生を許可して再生を実行するようにする再生処理手段と、を備えるデータ記録再生装置。

【請求項 3 5】請求項 3 4 に記載のデータ記録再生装置において、

前記使用者識別情報が予め記憶された不揮発性メモリを備え、

前記第 1 の使用者識別情報取得手段と、前記第 2 の使用者識別情報取得手段とでは、前記不揮発性メモリから、前記使用者識別情報を読み出して取得することを特徴とするデータ記録再生装置。

【請求項 3 6】請求項 3 4 に記載のデータ記録再生装置において、

前記第 1 の使用者識別情報取得手段と、前記第 2 の使用者識別情報取得手段とでは、記録ないし再生装置とは別体の使用者識別情報提供装置から、前記使用者識別情報を取得することを特徴とするデータ記録再生装置。

【請求項 3 7】請求項 3 4 に記載のデータ記録再生装置において、

前記第 1 の使用者識別情報取得手段は、記録ないし再生装置とは別体の使用者識別情報提供装置から、前記使用者識別情報を取得し、

前記第 2 の使用者識別情報取得手段は、前記使用者識別情報が予め記憶された不揮発性メモリから、前記使用者識別情報を読み出して取得することを特徴とするデータ記録再生装置。

【請求項 3 8】請求項 3 4 に記載のデータ記録再生装置において、

前記記録処理手段は、前記記録データを暗号化して記録する手段を備え、

前記再生処理手段は、前記記録媒体からの情報から検出された前記使用者識別情報と、前記第 2 の使用者識別情報取得手段により取得した前記使用者識別情報とが一致したときに、前記暗号化を解除する手段を備えることを特徴とするデータ記録再生装置。

10

20

30

40

50

【請求項 3 9】請求項 3 4 に記載のデータ記録再生装置において、

前記記録データの暗号化は、前記第 1 の使用者識別情報取得手段で取得された前記使用者識別情報に関連付けられたものであることを特徴とするデータ記録再生装置。

【請求項 4 0】請求項 3 4 に記載のデータ記録再生装置において、

前記第 1 の使用者識別情報取得手段で、前記使用者識別情報が取得できないときには、前記記録データの記録を不可とすることを特徴とするデータ記録再生装置。

【請求項 4 1】請求項 3 6 または請求項 3 7 に記載のデータ記録再生装置において、

前記使用者識別情報提供装置からの前記使用者識別情報は、暗号化されていることを特徴とするデータ記録再生装置。

【請求項 4 2】請求項 3 6 または請求項 3 7 に記載のデータ記録再生装置において、

前記使用者識別情報提供装置からの前記使用者識別情報は、予め前記使用者識別情報提供装置に格納された当該装置ごとに固有の情報であることを特徴とするデータ記録再生装置。

【請求項 4 3】請求項 3 4 に記載のデータ記録再生装置において、

前記使用者識別情報は、指紋、声紋、脈などの生体情報であることを特徴とするデータ記録再生装置。

【請求項 4 4】請求項 3 4 に記載のデータ記録再生装置において、

前記記録データと共に前記記録媒体に記録する前記使用者識別情報は、前記記録データに埋め込むことを特徴とするデータ記録再生装置。

【請求項 4 5】記録対象データに付随する使用者を特定するための使用者識別情報と、前記使用者識別情報とは別個に用意された使用者識別情報とが一致したときに前記記録対象データの記録を許可し、

前記記録対象データと共に、前記使用者識別情報を、記録媒体に記録することを特徴とするデータ記録方法。

【請求項 4 6】請求項 4 5 に記載のデータ記録方法において、

前記記録対象データおよび前記記録対象データに付随する使用者識別情報は、記録媒体から読み出されたものであることを特徴とするデータ記録方法。

【請求項 4 7】請求項 4 5 に記載のデータ記録方法において、

前記記録対象データに付随する使用者識別情報は、前記記録対象データから抽出されるものであることを特徴とするデータ記録方法。

【請求項 4 8】請求項 4 5 に記載のデータ記録方法において、

前記記録対象データに付随する使用者識別情報は、前記記録対象データと共に伝送路を通じて伝送されてくるこ

とを特徴とするデータ記録方法。

【請求項 49】請求項 45 に記載のデータ記録方法において、

前記予め用意された使用者識別情報は、不揮発性メモリに記憶されていることを特徴とするデータ記録方法。

【請求項 50】請求項 45 に記載のデータ記録方法において、

前記予め用意された使用者識別情報は、記録装置とは別体の使用者識別情報提供装置から取得することを特徴とするデータ記録方法。

【請求項 51】請求項 50 に記載のデータ記録方法において、

前記使用者識別情報提供装置が前記記録装置に接続されていないときには、前記記録対象データの記録を不可とすることを特徴とするデータ記録方法。

【請求項 52】請求項 50 に記載のデータ記録方法において、

前記使用者識別情報提供装置からの前記使用者識別情報は、暗号化して、前記記録装置に供給するようにすることを特徴とするデータ記録方法。

【請求項 53】請求項 50 に記載のデータ記録方法において、

前記使用者識別情報提供装置からの前記使用者識別情報は、予め前記使用者識別情報提供装置に格納された当該装置ごとに固有の情報であることを特徴とするデータ記録方法。

【請求項 54】請求項 45 に記載のデータ記録方法において、

前記使用者識別情報は、指紋、声紋、脈などの生体情報であることを特徴とするデータ記録方法。

【請求項 55】請求項 45 に記載のデータ記録方法において、

前記使用者識別情報は、前記記録対象データに埋め込んで前記記録媒体に記録することを特徴とするデータ記録方法。

【請求項 56】記録対象データに付随する使用者を特定するための使用者識別情報と、前記使用者識別情報とは別個に用意された使用者識別情報とが一致したときに前記記録対象データの記録を許可する制御手段と、

前記制御手段により記録が許可されたときに、前記記録対象データと共に、前記使用者識別情報を、記録媒体に記録することを特徴とするデータ記録装置。

【請求項 57】請求項 56 に記載のデータ記録装置において、

前記記録対象データおよび前記記録対象データに付随する使用者識別情報は、記録媒体から読み出されたものであって、前記使用者識別情報を検出する手段を備えることを特徴とするデータ記録装置。

【請求項 58】請求項 56 に記載のデータ記録装置において、

前記記録対象データに付随する使用者識別情報を、前記記録対象データから抽出する手段を備えることを特徴とするデータ記録装置。

【請求項 59】請求項 56 に記載のデータ記録装置において、

前記記録対象データに付随する使用者識別情報は、前記記録対象データと共に伝送路を通じて伝送されてくるものであって、前記伝送されてくる信号中から前記使用者識別情報を検出する手段を備えることを特徴とするデータ記録装置。

【請求項 60】請求項 56 に記載のデータ記録装置において、

前記予め用意された使用者識別情報は、不揮発性メモリに記憶されていることを特徴とするデータ記録装置。

【請求項 61】請求項 56 に記載のデータ記録装置において、

前記予め用意された使用者識別情報は、記録装置とは別体の使用者識別情報提供装置から取得することを特徴とするデータ記録装置。

【請求項 62】請求項 61 に記載のデータ記録装置において、

前記使用者識別情報提供装置が前記記録装置に接続されていないときには、前記記録対象データの記録を不可とすることを特徴とするデータ記録装置。

【請求項 63】請求項 61 に記載のデータ記録装置において、

前記使用者識別情報提供装置からの前記使用者識別情報は、暗号化されており、前記暗号化を解除する手段を備えることを特徴とするデータ記録装置。

【請求項 64】請求項 61 に記載のデータ記録装置において、

前記使用者識別情報提供装置からの前記使用者識別情報は、予め前記使用者識別情報提供装置に格納された当該装置ごとに固有の情報であることを特徴とするデータ記録装置。

【請求項 65】請求項 56 に記載のデータ記録装置において、

前記使用者識別情報は、指紋、声紋、脈などの生体情報であることを特徴とするデータ記録装置。

【請求項 66】請求項 56 に記載のデータ記録装置において、

前記使用者識別情報は、前記記録対象データに埋め込んで前記記録媒体に記録することを特徴とするデータ記録装置。

【請求項 67】使用者を特定するための使用者識別情報を取得し、取得した前記使用者識別情報を、記録データと共に、記録媒体に記録することを特徴とするデータ記録方法。

【請求項 68】請求項 67 に記載のデータ記録方法において、

前記記録データは、前記使用者識別情報に関連付けられた暗号化が施されることを特徴とするデータ記録方法。

【請求項 69】請求項 67 に記載のデータ記録方法において、

記録装置とは別体の使用者識別情報提供装置から、前記使用者識別情報を前記記録装置に供給するようにし、前記使用者識別情報提供装置が前記記録装置に接続されていないときには、前記記録データの記録を不可とすることを特徴とするデータ記録方法。

【請求項 70】請求項 69 に記載のデータ記録方法において、

前記使用者識別情報提供装置からの前記使用者識別情報は、暗号化して、前記記録装置に供給するようにすることを特徴とするデータ記録方法。

【請求項 71】請求項 69 に記載のデータ記録方法において、

前記使用者識別情報提供装置からの前記使用者識別情報は、予め前記使用者識別情報提供装置に格納された当該装置ごとに固有の情報であることを特徴とするデータ記録方法。

【請求項 72】請求項 67 に記載のデータ記録方法において、

前記使用者識別情報は、指紋、声紋、脈などの生体情報であることを特徴とするデータ記録方法。

【請求項 73】請求項 67 に記載のデータ記録方法において、

前記使用者識別情報は、前記記録データに埋め込むことを特徴とするデータ記録方法。

【請求項 74】使用者を特定するための使用者識別情報を取得するための使用者識別情報取得手段と、前記使用者識別情報取得手段で取得した前記使用者識別情報を、所定の記録データと共に、記録媒体に記録する記録処理手段と、を備えるデータ記録装置。

【請求項 75】請求項 74 に記載のデータ記録装置において、

前記記録処理手段は、前記記録データを、前記使用者識別情報に関連付けた暗号化処理して記録する手段を備えることを特徴とするデータ記録装置。

【請求項 76】請求項 74 に記載のデータ記録装置において、

前記使用者識別情報取得手段は、別体の使用者識別情報提供装置からの前記使用者識別情報を取得する手段からなり、

前記使用者識別情報提供装置が接続されていないときには、前記記録処理手段による記録処理動作を不可とする制御手段を設けたことを特徴とするデータ記録装置。

【請求項 77】請求項 76 に記載のデータ記録装置において、

前記使用者識別情報提供装置からの前記使用者識別情報

は暗号化されており、前記使用者識別情報取得手段は、前記使用者識別情報の暗号化を解除する手段を備えることを特徴とするデータ記録装置。

【請求項 78】請求項 76 に記載のデータ記録装置において、

前記使用者識別情報提供装置からの前記使用者識別情報は、予め前記使用者識別情報提供装置に格納された当該装置ごとに固有の情報であることを特徴とするデータ記録装置。

【請求項 79】請求項 74 に記載のデータ記録装置において、

前記使用者識別情報は、指紋、声紋、脈などの生体情報であることを特徴とするデータ記録装置。

【請求項 80】請求項 74 に記載のデータ記録装置において、

前記使用者識別情報は、前記記録データに埋め込まれることを特徴とするデータ記録装置。

【請求項 81】使用者を特定するための使用者識別情報が、記録データと共に記録された記録媒体からの前記記録データの再生方法であって、

前記記録媒体からの情報から前記使用者識別情報を検出し、

前記検出した前記使用者識別情報と、前記記録媒体以外から取得した前記使用者識別情報とが一致しているかどうかを判定し、

一致しているときには、前記記録データの再生を許可することを特徴とするデータ再生方法。

【請求項 82】請求項 81 に記載のデータ再生方法において、

前記使用者識別情報が予め記憶された不揮発性メモリを設け、前記再生時には前記不揮発性メモリから読み出した前記使用者識別情報を、前記記録媒体以外から取得した前記使用者識別情報とすることを特徴とするデータ再生方法。

【請求項 83】請求項 81 に記載のデータ再生方法において、

再生装置とは別体の使用者識別情報提供装置から、前記使用者識別情報を前記再生装置に供給して、前記不揮発性メモリに記憶するようにすることを特徴とするデータ再生方法。

【請求項 84】請求項 83 に記載のデータ再生方法において、

前記使用者識別情報提供装置からの前記使用者識別情報は、暗号化して、前記記録装置に供給するようにすることを特徴とするデータ再生方法。

【請求項 85】請求項 83 に記載のデータ再生方法において、

前記使用者識別情報提供装置からの前記使用者識別情報は、予め前記使用者識別情報提供装置に格納された当該使用者識別情報提供装置ごとに固有の情報であることを

特徴とするデータ再生方法。

【請求項 86】請求項 81 に記載のデータ再生方法において、

前記記録データは、暗号化されており、
前記記録媒体からの情報から検出された前記使用者識別情報と、前記記録媒体以外から取得した前記使用者識別情報とが一致したときに、前記暗号化を解除することを特徴とするデータ再生方法。

【請求項 87】請求項 86 に記載のデータ再生方法において、

前記記録データの暗号化は、前記使用者識別情報に関連付けられていることを特徴とするデータ再生方法。

【請求項 88】請求項 81 に記載のデータ再生方法において、

前記使用者識別情報は、指紋、声紋、脈などの生体情報であることを特徴とするデータ再生方法。

【請求項 89】使用者を特定するための使用者識別情報が、記録データと共に記録された記録媒体からの前記記録データの再生装置であって、

前記記録媒体からの情報から前記使用者識別情報を検出する使用者識別情報検出手段と、

前記検出した前記使用者識別情報と、前記記録媒体以外から取得した前記使用者識別情報とが一致していると検出したときには、前記記録データの再生を許可する制御手段とを備えることを特徴とするデータ再生装置。

【請求項 90】請求項 89 に記載のデータ再生装置において、

前記使用者識別情報が予め記憶された不揮発性メモリを備え、

前記不揮発性メモリから読み出した前記使用者識別情報を、前記記録媒体以外から取得した前記使用者識別情報とすることを特徴とするデータ再生装置。

【請求項 91】請求項 89 に記載のデータ再生装置において、

再生装置とは別体の使用者識別情報提供装置からの前記使用者識別情報を取得して、前記不揮発性メモリに記憶するようにする手段を備えることを特徴とするデータ再生装置。

【請求項 92】請求項 91 に記載のデータ再生装置において、

前記使用者識別情報提供装置からの前記使用者識別情報は暗号化されており、前記使用者識別情報の暗号化を解除する手段を備えることを特徴とするデータ再生装置。

【請求項 93】請求項 91 に記載のデータ再生装置において、

前記使用者識別情報提供装置からの前記使用者識別情報は、予め前記使用者識別情報提供装置に格納された当該装置ごとに固有の情報であることを特徴とするデータ再生装置。

【請求項 94】請求項 89 に記載のデータ再生装置にお

いて、

前記記録データは、暗号化されており、

前記記録媒体からの情報から検出された前記使用者識別情報と、前記記録媒体以外から取得した前記使用者識別情報とが一致したときに、前記暗号化を解除可能とすることを特徴とするデータ再生装置。

【請求項 95】請求項 94 に記載のデータ再生装置において、

前記記録データの暗号化は、前記使用者識別情報に関連付けられていることを特徴とするデータ再生装置。

【請求項 96】請求項 89 に記載のデータ再生装置において、

前記使用者識別情報は、指紋、声紋、脈などの生体情報であることを特徴とするデータ再生装置。

【請求項 97】請求項 1 に記載のデータ記録再生方法において、

前記記録データの再生時において、前記記録媒体からの情報から前記使用者識別情報が検出できなかったときには、前記記録媒体からの情報から抽出される再生条件にしたがった処理を行なうことを特徴とするデータ記録再生方法。

【請求項 98】請求項 1 に記載のデータ記録再生方法において、

前記記録データの再生時において、前記記録媒体からの情報から前記使用者識別情報が検出できなかったときには、制限付きで再生を行なうことを特徴とするデータ記録再生方法。

【請求項 99】請求項 1 に記載のデータ記録再生方法において、

前記記録データの再生時において、前記記録媒体からの情報から前記使用者識別情報が検出できなかったときには、課金を伴う再生のみを許可することを特徴とするデータ記録再生方法。

【請求項 100】請求項 1 に記載のデータ記録再生方法において、

前記記録データの再生時において、前記記録媒体からの情報から前記使用者識別情報が検出できなかったときには、再生を不可とすることを特徴とするデータ記録再生方法。

【請求項 101】請求項 1 に記載のデータ記録再生方法において、

前記記録データの再生時において、前記記録媒体からの情報から検出された前記使用者識別情報と、前記記録媒体以外から取得した前記使用者識別情報とが一致しなかったときは、前記記録媒体からの情報から抽出される再生条件にしたがった処理を行なうことを特徴とするデータ記録再生方法。

【請求項 102】請求項 1 に記載のデータ記録再生方法において、

前記記録データの再生時において、前記記録媒体からの

情報から検出された前記使用者識別情報と、前記記録媒体以外から取得した前記使用者識別情報とが一致しなかったときは、制限付きで再生を行なうことを特徴とするデータ記録再生方法。

【請求項 103】請求項 1 に記載のデータ記録再生方法において、

前記記録データの再生時において、前記記録媒体からの情報から検出された前記使用者識別情報と、前記記録媒体以外から取得した前記使用者識別情報とが一致しなかったときは、課金を伴う再生のみを許可することを特徴とするデータ記録再生方法。

【請求項 104】請求項 1 に記載のデータ記録再生方法において、

前記記録データの再生時において、前記記録媒体からの情報から検出された前記使用者識別情報と、前記記録媒体以外から取得した前記使用者識別情報とが一致しなかったときは、再生を不可とすることを特徴とするデータ記録再生方法。

【請求項 105】請求項 23 に記載のデータ記録再生装置において、

前記制御手段は、前記記録媒体からの情報から前記使用者識別情報が検出できなかったときに、前記記録媒体からの情報から抽出される再生条件にしたがった処理を行なうように制御することを特徴とするデータ記録再生装置。

【請求項 106】請求項 23 に記載のデータ記録再生装置において、

前記制御手段は、前記記録媒体からの情報から前記使用者識別情報が検出できなかったときには、制限付きで再生を行なうように制御することを特徴とするデータ記録再生装置。

【請求項 107】請求項 23 に記載のデータ記録再生装置において、

前記制御手段は、前記記録媒体からの情報から前記使用者識別情報が検出できなかったときには、課金を伴う再生のみを許可することを特徴とするデータ記録再生装置。

【請求項 108】請求項 23 に記載のデータ記録再生装置において、

前記制御手段は、前記記録媒体からの情報から前記使用者識別情報が検出できなかったときには、再生を不可とすることを特徴とするデータ記録再生装置。

【請求項 109】請求項 23 に記載のデータ記録再生装置において、

前記制御手段は、前記記録媒体からの情報から検出された前記使用者識別情報と、前記記録媒体以外から取得した前記使用者識別情報とが一致しなかったときは、前記記録媒体からの情報から抽出される再生条件にしたがって処理を行なうように制御することを特徴とするデータ記録再生装置。

【請求項 110】請求項 23 に記載のデータ記録再生装置において、

前記制御手段は、前記記録媒体からの情報から検出された前記使用者識別情報と、前記記録媒体以外から取得した前記使用者識別情報とが一致しなかったときは、制限付きで再生を行なうように制御することを特徴とするデータ記録再生装置。

【請求項 111】請求項 23 に記載のデータ記録再生装置において、

10 前記制御手段は、前記記録媒体からの情報から検出された前記使用者識別情報と、前記記録媒体以外から取得した前記使用者識別情報とが一致しなかったときは、課金を伴う再生のみを許可するように制御することを特徴とするデータ記録再生装置。

【請求項 112】請求項 23 に記載のデータ記録再生装置において、

20 前記制御手段は、前記記録媒体からの情報から検出された前記使用者識別情報と、前記記録媒体以外から取得した前記使用者識別情報とが一致しなかったときは、再生を不可とすることを特徴とするデータ記録再生装置。

【請求項 113】請求項 45 に記載のデータ記録方法において、

前記記録対象データに付随する使用者を特定するための使用者識別情報が検出できなかったときには、前記記録対象データに付随して得られる記録条件にしたがった処理を行なうことを特徴とするデータ記録方法。

【請求項 114】請求項 45 に記載のデータ記録方法において、

30 前記記録対象データに付随する使用者を特定するための使用者識別情報が検出できなかったときには、課金を伴う記録のみを許可することを特徴とするデータ記録方法。

【請求項 115】請求項 45 に記載のデータ記録方法において、

前記記録対象データに付随する使用者を特定するための使用者識別情報が検出できなかったときには、記録を不可とすることを特徴とするデータ記録方法。

【請求項 116】請求項 45 に記載のデータ記録方法において、

40 前記記録対象データに付随する使用者を特定するための使用者識別情報と、前記使用者識別情報とは別個に用意された使用者識別情報とが一致しなかったときには、前記記録対象データに付随して得られる記録条件にしたがった処理を行なうことを特徴とするデータ記録方法。

【請求項 117】請求項 45 に記載のデータ記録方法において、

50 前記記録対象データに付随する使用者を特定するための使用者識別情報と、前記使用者識別情報とは別個に用意された使用者識別情報とが一致しなかったときには、課金を伴う記録のみを許可することを特徴とするデータ記録

録方法。

【請求項 118】請求項 45 に記載のデータ記録方法において、前記記録対象データに付随する使用者を特定するための使用者識別情報と、前記使用者識別情報とは別個に用意された使用者識別情報とが一致しなかったときには、記録を不可とすることを特徴とするデータ記録方法。

【請求項 119】請求項 56 に記載のデータ記録装置において、前記制御手段は、前記記録対象データに付随する使用者を特定するための使用者識別情報が検出できなかったときには、前記記録対象データに付随して得られる記録条件にしたがった処理を行なうことを特徴とするデータ記録装置。

【請求項 120】請求項 56 に記載のデータ記録装置において、前記制御手段は、前記記録対象データに付随する使用者を特定するための使用者識別情報が検出できなかったときには、課金を伴う記録のみを許可することを特徴とするデータ記録装置。

【請求項 121】請求項 56 に記載のデータ記録装置において、前記制御手段は、前記記録対象データに付随する使用者を特定するための使用者識別情報が検出できなかったときには、記録を不可とすることを特徴とするデータ記録装置。

【請求項 122】請求項 81 に記載のデータ再生方法において、前記記録媒体からの情報から前記使用者識別情報が検出できなかったときには、前記記録媒体からの情報から抽出される再生条件にしたがって処理を行なうことを特徴とするデータ再生方法。

【請求項 123】請求項 81 に記載のデータ再生方法において、前記記録媒体からの情報から前記使用者識別情報が検出できなかったときには、制限付きで再生を行なうことを特徴とするデータ再生方法。

【請求項 124】請求項 81 に記載のデータ再生方法において、前記記録媒体からの情報から前記使用者識別情報が検出できなかったときには、課金を伴う再生のみを許可することを特徴とするデータ再生方法。

【請求項 125】請求項 81 に記載のデータ再生方法において、前記記録媒体からの情報から前記使用者識別情報が検出できなかったときには、再生を不可とすることを特徴とするデータ再生方法。

【請求項 126】請求項 81 に記載のデータ再生方法において、前記記録媒体からの情報から検出された前記使用者識別

情報と、前記記録媒体以外から取得した前記使用者識別情報とが一致しなかったときは、前記記録媒体からの情報から抽出される再生条件にしたがった処理を行なうことを特徴とするデータ再生方法。

【請求項 127】請求項 81 に記載のデータ再生方法において、

前記記録媒体からの情報から検出された前記使用者識別情報と、前記記録媒体以外から取得した前記使用者識別情報とが一致しなかったときは、制限付きで再生を行なうことを特徴とするデータ再生方法。

【請求項 128】請求項 81 に記載のデータ再生方法において、

前記記録媒体からの情報から検出された前記使用者識別情報と、前記記録媒体以外から取得した前記使用者識別情報とが一致しなかったときは、課金を伴う再生のみを許可することを特徴とするデータ再生方法。

【請求項 129】請求項 81 に記載のデータ再生方法において、

前記記録媒体からの情報から検出された前記使用者識別情報と、前記記録媒体以外から取得した前記使用者識別情報とが一致しなかったときは、再生を不可とすることを特徴とするデータ再生方法。

【請求項 130】請求項 89 に記載のデータ再生装置において、

前記制御手段は、前記記録媒体からの情報から前記使用者識別情報が検出できなかったときに、前記記録媒体からの情報から抽出される再生条件にしたがった処理を行なうように制御することを特徴とするデータ再生装置。

【請求項 131】請求項 89 に記載のデータ再生装置において、

前記制御手段は、前記記録媒体からの情報から前記使用者識別情報が検出できなかったときには、制限付きで再生を行なうように制御することを特徴とするデータ再生装置。

【請求項 132】請求項 89 に記載のデータ再生装置において、

前記制御手段は、前記記録媒体からの情報から前記使用者識別情報が検出できなかったときには、課金を伴う再生のみを許可することを特徴とするデータ再生装置。

【請求項 133】請求項 89 に記載のデータ再生装置において、

前記制御手段は、前記記録媒体からの情報から前記使用者識別情報が検出できなかったときには、再生を不可とすることを特徴とするデータ再生装置。

【請求項 134】請求項 89 に記載のデータ再生装置において、

前記制御手段は、前記記録媒体からの情報から検出された前記使用者識別情報と、前記記録媒体以外から取得した前記使用者識別情報とが一致しなかったときは、前記記録媒体からの情報から抽出される再生条件にしたが

て処理を行なうように制御することを特徴とするデータ再生装置。

【請求項 135】請求項 89 に記載のデータ再生装置において、

前記制御手段は、前記記録媒体からの情報から検出された前記使用者識別情報と、前記記録媒体以外から取得した前記使用者識別情報とが一致しなかったときは、制限付きで再生を行なうように制御することを特徴とするデータ再生装置。

【請求項 136】請求項 89 に記載のデータ再生装置において、

前記制御手段は、前記記録媒体からの情報から検出された前記使用者識別情報と、前記記録媒体以外から取得した前記使用者識別情報とが一致しなかったときは、課金を伴う再生のみを許可するように制御することを特徴とするデータ再生装置。

【請求項 137】請求項 89 に記載のデータ再生装置において、

前記制御手段は、前記記録媒体からの情報から検出された前記使用者識別情報と、前記記録媒体以外から取得した前記使用者識別情報とが一致しなかったときは、再生を不可とすることを特徴とするデータ再生装置。

【請求項 138】記録データと共に、使用者を特定するための使用者識別情報が記録されていることを特徴とする記録媒体。

【請求項 139】前記使用者識別情報は、前記記録データ中に埋め込まれていることを特徴とする請求項 138 に記載の記録媒体。

【請求項 140】前記記録データは、前記使用者識別情報に関連付けられた暗号化処理がなされて記録されていることを特徴とする請求項 138 に記載の記録媒体。

【請求項 141】前記使用者識別情報は、指紋、声紋、脈などの生体情報であることを特徴とする請求項 138 に記載の記録媒体。

【請求項 142】著作権管理を必要とするデータ中に、使用者を特定するための使用者識別情報が含まれてなる伝送データ。

【請求項 143】前記使用者識別情報は、前記データ中に埋め込まれていることを特徴とする請求項 142 に記載の伝送データ。

【請求項 144】前記データは、前記使用者識別情報に関連付けられた暗号化処理がなされていることを特徴とする請求項 142 に記載の伝送データ。

【請求項 145】使用者を特定するための使用者識別情報を含む伝送データを伝送し、前記伝送データの受信時に、前記伝送データから前記使用者識別情報を検出し、その検出した前記使用者識別情報と、前記伝送データ以外から取得した前記使用者識別情報とを比較し、一致したときに、前記伝送データを利用可能とすることを特徴とするデータ伝送方法。

【請求項 146】前記使用者識別情報は、前記伝送データ中に埋め込まれていることを特徴とする請求項 145 に記載のデータ伝送方法。

【請求項 147】前記伝送データは、暗号化されており、前記使用者識別情報と、前記伝送データ以外から取得した前記使用者識別情報とが一致したときに、前記暗号化解除可能とすることを特徴とする請求項 145 に記載のデータ伝送方法。

【請求項 148】前記伝送データの暗号化は、前記使用者識別情報に関連付けられていることを特徴とする請求項 147 に記載のデータ伝送方法。

【請求項 149】前記使用者識別情報は、指紋、声紋、脈などの生体情報であることを特徴とする請求項 145 に記載のデータ伝送方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、著作権管理が必要なコンテンツデータ、例えば、オーディオ情報、画像情報、ゲームプログラムおよびデータ、コンピュータプログラムなどのデータを記録、再生する方法、装置に関する。

【0002】

【従来の技術】デジタルコンテンツの普及に伴い、このデジタルコンテンツについての不正な複製（コピー）による著作権侵害が問題となっている。すなわち、テープ媒体などへのアナログ記録の場合には、オーディオデータや画像データがアナログ的に記録されるため、複製を行なうと品質が劣化する。これに対し、デジタル的にオーディオデータや画像データを記録し再生する機器においては、原理的に複製によって情報品質が劣化することがなく、複製を多数回繰り返すことさえも品質の劣化無しに可能である。

【0003】そのため、デジタル的に処理を行なう機器による不正コピーによる損害は、アナログの場合よりさらに大きなものとなり、デジタル的に処理を行なう機器における不正コピー防止は、非常に重要になっている。

【0004】そこで、この問題に対処するため、デジタルコンテンツに複製制御のための情報を付加し、この付加情報を用いて、不正な複製を防止することが行われている。

【0005】例えば、この複製の防止のための制御として、オーディオコンテンツについては、1回は複製を認めるが、1回複製されたものからの複製を禁止するSCMS (Serial Copy Management System) と呼ばれる世代制限の複製制御方式による著作権保護施策が、CD (コンパクトディスク)、MD (ミニディスク (登録商標))、DAT (デジタルオーディオテープ) などにおいて用いられている。

【0006】このSCMS方式の複製制御方式について、図13を参照して説明する。

【0007】例えば、ディスク1には、オリジナルソースのオーディオ信号がデジタル記録されている。デジタルオーディオ信号は、ディスク1に、所定の記録フォーマットで記録されており、SCMS方式による1回複製可能を示す付加情報が、例えばデジタル信号中の特定のエリアに記録されている。

【0008】再生装置2は、ディスク1から読み出した信号からデジタルオーディオ信号を再生し、前記の付加情報と共に、記録装置3に伝送する。再生装置2では、通常再生速度（1倍速）に等しい時間分をかけて、デジタルオーディオ信号を記録装置3に伝送する。

【0009】このデジタルオーディオ信号を受け取った記録装置3は、デジタルオーディオ信号の付加情報が1回複製可能であるときには、入力デジタル信号の複製が可能であると認識する。記録装置3は、付加情報が1回複製可能であることを確認すると、記録可能なディスク4にデジタル信号を複製記録する。その際に、記録装置3は、付加情報を「1回複製可能」の状態から、「複製禁止」の状態に書き換える。したがって、ディスク4には、デジタル信号が複製記録が行われると共に、その付加情報として、「複製禁止」の情報が記録される。

【0010】この1回目の複製記録が行われたディスク4（第1世代のディスク）が再生装置5で再生されて、記録装置6に供給された場合、記録装置6では、付加情報が「複製禁止」となっていることを検知するので、記録可能なディスク7への記録はできなくなる。

【0011】このときの複製速度は、再生装置2からのオーディオ信号の伝送速度と等しくなり、オーディオ信号を標準再生時間で再生するとき、すなわち、ノーマル再生速度に等しい速度となる。

【0012】ここで、標準再生時間とは、オーディオ信号の場合、実時間再生速度であり、人間が通常知覚するときの再生速度である。例えば、データの場合、標準再生速度は各再生機器により決定され、人間の知覚に関わるものではない。

【0013】以上のようにして、SCMS方式では、記録装置で第1世代の複製は許可するが、第1世代の媒体からの第2世代の複製はできないように制御して、著作権保護を行っている。

【0014】

【発明が解決しようとする課題】SCMS方式の本来の趣旨は、第2世代の複製を禁止することにより、業としての大量の複製が行なわれてしまうのを防止することにある。現在、一般化している「個人使用の範囲内での複製は自由」という著作権についての概念を否定するものではない。

【0015】ところで、最近では、MD（ミニディスク（登録商標））プレーヤや、カード型メモリプレーヤなどのように、記録再生メディアとして種々のものが登場しており、ユーザも、その日の気分によって、再生メ

ディアとして、MDを用いたり、カード型メモリを用いたりするようになってきている。このような現状では複製が頻繁に行なわれるようになるが、常にオリジナルのメディアからしか複製をすることができないSCMS方式では、個人使用の範囲内での複製であるにもかかわらず、不便を来たしてしまう。

【0016】また、最近のパーソナルコンピュータは、CDプレーヤの機能を備え、ハードディスクにCDの音楽情報を格納（複製）して再生できるようになっている。カード型メモリへの複製は、複製速度が速いことから、パーソナルコンピュータのハードディスクからの複製が便利であるが、厳密には、ハードディスクからの複製は、第2世代になり、その複製はできないことになる。

【0017】この発明は、以上の点にかんがみ、SCMS方式を採用することなく、個人使用の範囲での複製は自由にし、かつ、業とした不正な複製を有効に防止することができる方法および装置を提供することを目的とする。

【0018】

【課題を解決するための手段】上記課題を解決するため、請求項1の発明によるデータ記録再生方法は、記録データの記録時には、使用者を特定するための使用者識別情報を、前記記録データと共に、記録媒体に記録し、前記記録データの再生時には、前記記録媒体からの情報から検出された前記使用者識別情報と、前記記録媒体以外から取得した前記使用者識別情報とが一致したときは、前記記録データの再生を許可することを特徴とする。

【0019】上記の請求項1の発明によれば、使用者識別情報が、記録データと共に、記録媒体に記録されている。そして、再生時には、記録媒体からの情報から検出された使用者識別情報が、記録媒体以外から取得した前記使用者識別情報と比較され、一致したときには、その記録データは、その再生装置の使用者が所有しているものであるとして認識され、再生可能とされる。

【0020】したがって、個人使用の範囲内での複製が自由になると共に、業として不正な複製が行なわれたときには、その複製により作成された記録媒体からの情報から検出された使用者識別情報と、再生装置の使用者の使用者識別情報とが再生時に不一致になることから、再生ができなくなり、業としての不正な複製を実質的に防止することができる。

【0021】また、請求項5の発明は、請求項1に記載のデータ記録再生方法において、前記記録データの記録時には、記録装置とは別体の使用者識別情報提供装置から、前記使用者識別情報を前記記録装置に供給するようにし、前記使用者識別情報提供装置が前記記録装置に接続されていないときには、前記記録データの記録を不可とすることを特徴とする。

【0022】この請求項5の発明によれば、使用者識別情報提供装置が記録装置に接続されていないときには、記録ができないようにされているので、記録時には、必ず、記録データと共に、使用者識別情報が記録媒体に記録される。したがって、再生時の、使用者識別情報を用いた再生制御と相俟って、個人使用の範囲内の複製にとどめることができる。

【0023】さらに請求項6の発明は、請求項5に記載のデータ記録再生方法において、前記使用者識別情報が予め記憶された不揮発性メモリを設け、前記不揮発性メモリから読み出した前記使用者識別情報を、前記記録媒体以外から取得した前記使用者識別情報とすることを特徴とする。

【0024】この請求項6の発明によれば、請求項5の要件により、記録時に記録データと共に使用者識別情報が記録媒体に確実に記録されて、使用者の制限が厳格に行われる代わりに、再生側では、不揮発性メモリに予め登録した使用者識別情報を用いて、記録媒体からの使用者識別情報と比較することができる。したがって、使用者は、再生時には、記録時のような使用者識別情報提供装置を、再生装置に接続しなくても再生出力を得ることができ、使い勝手がよくなる。

【0025】

【発明の実施の形態】以下、この発明によるデータ記録・再生方法および装置の実施の形態を、ディスク記録媒体にオーディオ信号を記録し、再生する場合を例にとりて、図を参照しながら説明する。

【0026】図1は、この発明によるデータ記録再生装置の第1の実施の形態を用いた記録再生システムのブロック図である。

【0027】この第1の実施の形態のシステムにおいては、図1に示すように、実施の形態のデータ記録再生装置10と、使用者識別情報提供装置20とからなる。使用者識別情報提供装置は、以下の説明においては、ユーザIDモジュールと称する。この実施の形態においては、データ記録再生装置10には、ユーザIDモジュール20を接続するための端子が、必ず付いている。この端子を通じて、データ記録再生装置10とユーザIDモジュール20との間でやり取りする情報は、すべて暗号化される。

【0028】データ記録再生装置10は、記録再生用信号処理部（以下、記録再生エンジンチップと称する）11と、記録／再生装置部12と、システム制御部13と、不揮発性メモリ14と、入力操作部15と、表示部16とを備えている。記録再生エンジンチップ11は、機能的には、記録エンコード／再生デコード処理部111と、ユーザIDモジュール20との間で、暗号化を伴う通信パスを確立して通信を行なうための暗号処理部112と、制御部113とを備えて構成されている。

【0029】そして、記録再生エンジンチップ11の記

録エンコード／再生デコード処理部111は、システム制御部13の制御を受けて、記録時には、これに対して入力されるアナログオーディオ信号あるいはデジタルオーディオ信号を、後述のように記録エンコード処理して、記録／再生装置部12に出力し、また、再生時には、記録／再生装置部12からの再生データを後述のように再生デコードして、アナログオーディオ信号あるいはデジタルオーディオ信号として出力する。

【0030】また、記録再生エンジンチップ11の暗号化処理部112は、ユーザIDモジュール20に対して、この例では、ケーブル40を通じて接続される。この場合、暗号化処理部112は、システム制御部13の制御の下、ユーザIDモジュール20との間で認証作業を行う認証機能を備え、認証がとれたときに、ユーザIDモジュール20との間に通信路を確立する。この場合に、確立した通信路を伝送するデータは暗号化するものであるので、通信を行なう前に、その暗号化および暗号解除のための暗号鍵の伝達を行なう。

【0031】また、記録再生エンジンチップ11の制御部113は、システム制御部13からの制御信号に応じて記録エンコード／再生デコード処理部111と、暗号処理部112を動作制御すると共に、この制御部113に対して接続される不揮発性メモリ14に対する使用者識別情報の、書き込み、読み出しを制御する。

【0032】記録／再生装置部12は、システム制御部13による制御を受けて、記録再生エンジンチップ11からの記録信号を、ディスク30に記録し、また、ディスク30から読み出したデータを、記録再生エンジンチップ11に供給する。

【0033】システム制御部13は、入力操作部15を通じた使用者の入力指示に従った制御を行ない、また、必要な表示用データを表示部16に送って、その画面に表示する。表示部16の表示素子としては、液晶ディスプレイなどが用いられる。

【0034】ユーザIDモジュール20は、一つのデータ記録再生装置10に、一つ付属するもので、使用者識別情報（以下、ユーザIDという）をデータ記録再生装置10に供給するものである。ユーザIDモジュール20は、暗号処理および制御部（以下、セキュアチップと称する）21と、不揮発性メモリ22と、入力操作部23と、表示部24とを備えて構成されている。

【0035】セキュアチップ21は、記録再生エンジンチップ11との間で認証作業を行う機能を備え、認証がとれたときに、記録再生エンジンチップ11との間に通信路を確立する。この際に、通信路を伝送するデータは暗号化するものであるので、通信を行なう前に、暗号化および暗号解除のための暗号鍵の伝達を行なう。

【0036】不揮発性メモリ22には、予め工場出荷時に、各ユーザIDモジュール20に固有のモジュール識別情報（以下、モジュールIDと称する）、例えば固有

の数値が書き込まれている。

【0037】そして、使用者は、データ記録再生装置10を購入したときに、それに付属しているユーザIDモジュール20に、入力操作部23を通じて、表示部24の画面で確認しながら、「ユーザ名」を入力して登録する。

【0038】[ユーザIDモジュール20へのユーザ名の登録]図2は、このユーザIDモジュール20への「ユーザ名」の登録のための処理手順を示すフローチャートである。

【0039】まず、ユーザIDモジュール20は、「ユーザ名」の入力するための画面を、表示部24に表示し、使用者に、ユーザIDモジュール20への「ユーザ名」の入力を促す(ステップS1)。これを受けて、使用者が、ユーザ名を入力すると、ユーザIDモジュール20は、そのユーザ名の入力完了を確認した後(ステップS2)、入力された「ユーザ名」を、不揮発性メモリ22に格納する。以上の処理は、セキュアチップ21が実行するものである。

【0040】なお、以上のようにして入力されて登録されたユーザ名は、入力操作部23を通じた登録ユーザ名の確認操作が行なわれたときに、不揮発性メモリ22から読み出されて、表示部24の画面に表示されて、確認することができるようにされている。

【0041】こうして、入力された「ユーザ名」と、不揮発性メモリ22に予め記憶されていた「モジュールID」とが、1対1に対応付けられることにより、実質的にモジュールIDがユーザIDとしての意味を有することになる。つまり、ユーザIDは、この明細書においては、モジュールIDとユーザ名との両方を含む概念を意味する場合と、モジュールIDのみからなる概念を意味する場合の2通りの場合がある。

【0042】[データ記録再生装置へのユーザIDの登録]以上のようにして、ユーザ名がユーザIDモジュール20に登録された後には、使用者は、ユーザIDモジュール20をデータ記録再生装置10に接続して、データ記録再生装置10に対するユーザID登録を行なう必要がある。

【0043】図3および図4は、ユーザIDモジュール20を用いて、データ記録再生装置10にユーザIDの登録をする処理手順を示すフローチャートである。図3は、このときの、ユーザIDモジュール20側での処理であり、また、図4は、データ記録再生装置10側での処理である。

【0044】<ユーザIDモジュール20側の処理動作>ユーザIDモジュール20では、図3に示すように、まず、データ記録再生装置10に接続されたかどうか判別する(ステップS11)。接続されていないと判別されたときには、データ記録再生装置10が接続されていないことを使用者に報知して、接続を促すようにする

(ステップS12)。

【0045】そして、データ記録再生装置10にユーザIDモジュール20が接続されていることが検知されたときには、使用者による入力操作部23を通じた「登録指示」を待ち(ステップS13)、登録指示が受け付けられたことを検知したときには、データ記録再生装置10の記録再生エンジンチップ11との間での認証確認すると共に、暗号鍵の伝達を行なう(ステップS14)。

【0046】そして、認証確認がとれて、通信路が確立できたか否か判別し(ステップS15)、認証ができずに、通信路が確立できなかったときには、表示部24にエラー表示をして(ステップS17)、この処理ルーチンを終了する。また、通信路が確立できたときには、不揮発性メモリ22からモジュールIDおよびユーザ名を読み出し、暗号化して、データ記録再生装置10に対して、登録命令と共に送信する(ステップS16)。

【0047】<データ記録再生装置10側の処理動作>一方、データ記録再生装置10側においては、図4に示すように、まず、ユーザIDモジュール20が接続されるのを待ち、接続されたことを判別すると(ステップS21)、記録再生エンジンチップ11は、ユーザIDモジュール20との間での認証確認すると共に、暗号鍵の伝達を行なう(ステップS22)。

【0048】そして、認証確認がとれて、通信路が確立できたか否か判別し(ステップS23)、認証ができずに、通信路が確立できなかったときには、表示部16にエラー表示をして(ステップS26)、この処理ルーチンを終了する。

【0049】また、通信路が確立できたときには、ユーザIDモジュール20からの「モジュールID」および「ユーザ名」を含む登録命令の受信を待ち(ステップS24)、受信を確認したら、記録再生エンジンチップ11は、不揮発性メモリ14に、受信したモジュールIDおよびユーザ名を格納して、所有者登録をする(ステップS25)。

【0050】なお、以上のようにして入力されて登録されたユーザ名は、入力操作部15を通じた登録ユーザ名の確認操作が行なわれたときに、不揮発性メモリ14から読み出されて、表示部16の画面に表示されて、確認することができるようにされている。

【0051】また、データ記録再生装置10のユーザIDは、一旦登録されたものであっても、ユーザIDモジュール20を用いて再登録することにより、別のユーザIDに設定し直すこともできる。

【0052】[データ記録再生装置10での録音処理動作]次に、データ記録再生装置10での録音処理動作を図5および図6のフローチャートを参照しながら説明する。

【0053】この実施の形態においては、録音をする際には、データ記録再生装置10には、ユーザIDモジュ

10

20

30

40

50

ール20を接続しておく必要がある。すなわち、データ記録再生装置10は、まず、ユーザIDモジュール20が接続されているかどうか判別する(ステップS31)。接続されていないと判別されたときには、ユーザIDモジュール20が接続されていないことを使用者に報知して、接続を促すようにする(ステップS32)。例えば「ユーザIDモジュールが接続されていないので記録はできません。ユーザIDモジュールを接続して下さい。」というメッセージを表示部16に表示したり、音声によるメッセージとして放音するようにする。

【0054】そして、データ記録再生装置10にユーザIDモジュール20が接続されていることが検知されたときには、使用者による入力操作部15を通じた「録音指示」を待ち(ステップS33)、「録音指示」が受け付けられたことを検知したときには、データ記録再生装置10のシステム制御部13は、録音命令を記録再生エンジンチップ11や記録/再生装置部12に発行し、録音開始準備状態とする(ステップS34)。

【0055】次に、記録再生エンジンチップ11は、ユーザIDモジュール20のセキュアチップ21との間での認証確認すると共に、暗号鍵の伝達を行なう(ステップS35)。そして、認証確認がとれて、通信路が確立できたか否かを判別し(ステップS36)、認証ができずに、通信路が確立できなかったときには、録音動作を中止し(ステップS37)、その後、表示部24にエラー表示をして(ステップS38)、この処理ルーチンを終了する。

【0056】また、ステップS36で、通信路が確立できたと判別したときには、記録再生エンジンチップ11は、ユーザIDモジュール20に対して、ユーザID、つまり、この例の場合には、モジュールIDおよびユーザ名の送信要求を出す(ステップS39)。

【0057】ユーザIDモジュール20のセキュアチップ21は、この送信要求に対して、不揮発性メモリ22からモジュールIDおよびユーザ名を読み出し、暗号化して、データ記録再生装置10に対して送信する。データ記録再生装置10の記録再生エンジンチップ11は、このモジュールIDおよびユーザ名の受信を確認する(ステップS40)。

【0058】次に、オーディオデータ中に埋め込まれているモジュールIDの検出を行ない(ステップS41)、モジュールIDが検出できたか否かを判別する(ステップS42)。そして、モジュールIDが検出できたときには、検出されたモジュールIDと、ユーザIDモジュール20から取得したモジュールIDとを比較照合する(ステップS43)。

【0059】その比較照合の結果、両モジュールIDが一致したか否かを判別し(ステップS44)、一致したときには、記録許可となり、入力オーディオデータを圧縮し、受信したユーザIDを暗号鍵とした暗号化処理する

(ステップS45)。

【0060】この場合、暗号鍵としては、ユーザ名のみを用いる場合、モジュールIDのみを用いる場合、またはユーザ名およびモジュールIDの両者を用いる場合のいずれであってもよい。

【0061】そして、この圧縮および暗号化処理したオーディオデータ中に、ユーザIDモジュール20から取得した「ユーザ名」と、「モジュールID」とを埋め込む(ステップS46)。この場合に、モジュールIDは暗号化して埋め込む。ユーザIDの秘匿性を高めるためである。ステップS46では、さらに、後述する記録ルールや再生ルールを、記録対象のオーディオデータに埋め込む。

【0062】以上のようにして、暗号化し、ユーザIDなどを埋め込んだオーディオデータは、記録媒体としてのディスク30に記録する(ステップS47)。

【0063】一方、ステップS42でモジュールIDが検出できなかったとき、ステップS44でオーディオデータから検出されたモジュールIDとユーザIDモジュール20からのモジュールIDとが不一致であったときには、オーディオデータ中に埋め込まれている記録条件(記録ルール)を検出し(ステップS48)、その検出した記録ルールにしたがった処理を行なう(ステップS49)。

【0064】この記録ルールの情報の埋め込み処理としては、電子透かし処理と呼ばれている処理や、その他の埋め込み処理を用いることができる。また、オーディオデータ中に埋め込むのではなく、TOC(Table Of Contents)などのオーディオデータとは別の記録エリアや、サブコードのエリアなどに記録するようにしてもよい。

【0065】このとき埋め込む記録ルールとしては、例えば、

R①「無料で記録(複製)可能」

R②「記録(複製)は有料」

R③「記録(複製)はフリー」

R④「記録(複製)は不可」

のうちの一つが選択されて記録されているものである。記録ルールの記録情報としては、記録ルールの内容そのものを記録してもよいが、上述のR①～R④のいずれであるかの情報を記録することもできる。

【0066】ここで、上記R①「無料で記録(複製)可能」は、ユーザIDをオーディオデータに埋め込んで、記録を実行させるものである。これは、この例では、オーサリング装置でレコード会社などにより制作される読み出し専用形式(以下、ROMタイプという)のディスクなどの記録媒体には、所有者無しとしてユーザIDを埋め込まずに記録するので、このROMタイプの記録媒体からのオーディオデータの記録(複製)時の処理となる。

【0067】また、上記R②「記録（複製）は有料」は、課金処理が可能な記録装置において、課金処理が行ってきたときに記録を許可するものである。課金処理が不能の記録装置の場合には、記録は不可とされる。なお、課金処理の例については、後述する。

【0068】また、上記R③「記録（複製）はフリー」は、ユーザIDはオーディオデータに記録せずに、記録（複製）を行なう処理である。さらに、R④「記録（複製）は不可」は、全く記録（複製）は不可であることを意味している。

【0069】なお、上述のように、記録ルールは、ユーザIDが不一致の場合だけでなく、記録対象のオーディオデータからユーザIDが検出できなかったときにも適用されるが、ユーザIDが不一致の場合と、有効なユーザIDが得られない場合とでは、異なる記録ルールを記録しておくようにしてもよい。

【0070】また、後述するように、この実施の形態では、再生時には、オーディオデータ中に埋め込まれたユーザIDと、不揮発性メモリ14に格納されたユーザIDとの照合を行ない、両者が一致したときに、そのオーディオデータの再生が可能となる。そして、この実施の形態では、再生時にオーディオデータからユーザIDが検出できなかったとき、また、再生時での照合の結果、ユーザIDが不一致であるときに、どのように処理するか再生ルール（再生条件）も、ステップS46で、オーディオデータ中に埋め込むようにする。

【0071】この再生ルールの情報の埋め込み処理としては、記録ルールと同様に、電子透かし処理と呼ばれている処理や、その他の周知の埋め込み処理を用いることができる。また、オーディオデータ中に埋め込むのではなく、TOC (Table Of Contents) などのオーディオデータとは別の記録エリアや、サブコードのエリアなどに記録するようにしてもよい。

【0072】この再生時にユーザIDが不一致の場合の再生ルールとしては、例えば、

PB①「無料再生可能」

PB②「再生禁止（再生不可）」

PB③「再生は有料」

PB④「制限付きで再生可能」

のうちの一つが選択されて記録されるものである。再生ルールの記録情報としては、再生ルールの内容そのものを記録してもよいが、上述のPB①～PB④のいずれであるかの情報を記録することもできる。

【0073】ここで、上記PB①「無料再生可能」の場合には、再生装置に登録されたユーザIDに関係なく、常に、再生可能可能となり、PB②「再生禁止（再生不可）」の場合には、再生装置に登録されたユーザIDに関係なく、常に、再生が禁止される。前述したように、この例では、オーサリング装置でレコード会社などにより制作されるROMタイプのディスクなどの記録媒体に

は、ユーザIDを埋め込まずに記録するので、再生オーディオデータから有効なユーザIDが得られない場合として、上記PB①のルールが記録される。

【0074】また、上記PB③「再生は有料」の場合には、課金処理が可能な再生装置において、課金処理が行ってきたときに再生を許可するものである。課金処理が不能の再生装置の場合には、再生は不可とされる。なお、課金処理の例については、後述する。

【0075】また、上記PB④「制限付きで再生可能」は、例えば、全部又は一部の試聴モードを許可し、その試聴モードの後には、上記PB②又はPB③のルールとするものである。ここで、試聴モードとは、

a) n回、例えば1回だけ無料再生可能

b) m秒分だけ無料再生可能

c) さわり部分やさび部分だけ無料再生可能

を意味する。

【0076】このPB④「制限付き再生可能」の再生ルールで、前記a)やb)を採用する場合には、再生装置は、例えば、ISRC (International Standard Recording Code) などのコンテンツID (識別コード) に対応させて、そのコンテンツIDで識別されるオーディオデータの試聴履歴の情報、例えば試聴回数や、試聴秒数などを記録するようにする。

【0077】この実施の形態では、後述の再生処理で説明するように、この再生ルールは、再生時にユーザIDが不一致の場合だけでなく、再生オーディオデータから、有効なユーザIDが得られないときにも共通に適用される。しかし、ユーザIDが不一致の場合と、有効なユーザIDが得られない場合とでは、異なる再生ルールを記録するようにしてもよい。

【0078】例えば、オーサリング装置でレコード会社などにより制作されるROMタイプのディスクなどの記録媒体にも、ユーザIDとして、例えば「ORIGINAL」などの特定のIDが記録される場合には、再生装置は、その特定のIDを検出したときには、自己の装置のユーザIDと不一致の場合でも、再生許可すべきである。したがって、再生ルールが埋め込まれるものとした場合には、その再生ルールは、「再生可能」とされる。

【0079】一方、このように特定のユーザIDが、ROMタイプのディスクなどの記録媒体の記録データに埋め込まれるなどして、前記記録データに付随して記録されると定められている場合には、再生装置において、有効なユーザIDが得られないときには、そのオーディオデータは、不正に記録されたものであるとすることができ。したがって、その時の再生ルールは再生不可とするのがよい。

【0080】しかし、オーサリング装置でレコード会社などにより制作されるROMタイプのディスクなどの記録媒体には、ユーザIDを記録しないと定められている

場合には、上述のような再生ルールのうちの一つを共通に用いることができる。

【0081】[データ記録再生装置10での再生処理動作]次に、以上のようにして録音されたオーディオデータを、データ記録再生装置10で再生する場合の処理動作を図7および図8のフローチャートを参照しながら説明する。

【0082】まず、記録済みのディスクが装填されるのを待ち、装填されたことを判別すると(ステップS51)、記録再生エンジンチップ11は、使用者からの再生指示を待つ。そして、使用者からの再生指示を確認すると(ステップS52)、ディスクから再生指示のあったオーディオデータを読み出す(ステップS53)。

【0083】そして、読み出されたオーディオデータに埋め込まれているユーザIDを検出する。そして、ユーザIDのうちの、この例では、暗号化されているモジュールIDの暗号を解除して検出する(ステップS54)。そして、モジュールIDが検出できたか否か判別し(ステップS55)、検出できなかったときには、再生オーディオデータに埋め込まれている再生ルールを検出し(ステップS73)、その検出された再生ルールに従った処理を行なう(ステップS74)。

【0084】また、ステップS55で、モジュールIDを検出することができたと判別されたときには、その検出されたモジュールIDと、不揮発性メモリ14に記憶されているモジュールIDとを比較照合する(ステップS56)。

【0085】そして、両者が一致しているかどうか判別し(ステップS57)、一致しているときには、ユーザIDが用いられて暗号化されているオーディオデータの暗号を解き(ステップS58)、また、オーディオデータの圧縮を解凍する(ステップS59)。そして、オーディオデータを復号して、再生出力する(ステップS60)。

【0086】一方、ステップS57で、ディスク30から読み出したデータから検出されたモジュールIDと、不揮発性メモリ14から読み出されたモジュールIDとが不一致であると判別されたときには、ユーザに、ユーザIDモジュール20を接続させる設定になっているかどうかを判別し、ユーザIDモジュールを接続させる設定になっていなければ、再生オーディオデータに埋め込まれている再生ルールを検出し(ステップS73)、その検出された再生ルールに従った処理を行なう(ステップS74)。この例では、例えば再生禁止となる。

【0087】この場合の再生禁止には、正常な再生出力が行なわれないことも含まれる。つまり、再生出力としてノイズが出力される場合の他、再生出力に代えて、

「違法に複製された記録媒体からの再生である」旨のメッセージを、オーディオ出力として送出するようにしてもよい。

【0088】ステップS61で、ユーザに、ユーザIDモジュールを接続させる設定になっていると判別されたときには、データ記録再生装置10は、ユーザIDモジュール20が接続されているかどうか判別する(ステップS62)。接続されていないと判別されたときには、ユーザIDモジュール20が接続されていないことを使用者に報知して、接続を促すようにする(ステップS63)。

【0089】そして、データ記録再生装置10にユーザIDモジュール20が接続されていることが検知されたときには、記録再生エンジンチップ11は、ユーザIDモジュール20との間での認証確認すると共に、暗号鍵の伝達を行なう(ステップS64)。そして、認証確認がとれて、通信路が確立できたか否か判別し(ステップS65)、認証ができずに、通信路が確立できなかったときには、オーディオデータに埋め込まれた再生ルールに従った処理を行なう(ステップS73、ステップS74)。この例では、前述のように再生禁止となる。

【0090】また、ステップS65で、通信路が確立できたと判別したときには、記録再生エンジンチップ11は、ユーザIDモジュール20に対して、ユーザIDのうちの、この例の場合には、モジュールIDの送信要求を出す(ステップS66)。

【0091】ユーザIDモジュール20のセキュアチップ21は、この送信要求に対して、不揮発性メモリ22からモジュールIDを読み出し、暗号化して、データ記録再生装置10に対して送信する。データ記録再生装置10の記録再生エンジンチップ11は、このモジュールIDの受信を確認すると(ステップS67)、ディスク30から読み出したデータから検出されたモジュールIDと、受信し暗号を解除したモジュールIDとを比較照合する(ステップS68)。

【0092】そして、両者が一致しているかどうか判別し(ステップS69)、両者が不一致であったときには、オーディオデータに埋め込まれた再生ルールに従った処理を行なう(ステップS73、ステップS74)。前述したように、この例では、再生禁止となる。

【0093】また、両者が一致したときには、ユーザIDが用いられて暗号化されているオーディオデータの暗号を解き(ステップS70)、また、オーディオデータの圧縮を解凍する(ステップS71)。そして、オーディオデータを復号して、再生出力する(ステップS72)。

【0094】以上のようにして、この実施の形態においては、記録時に、登録されたユーザIDを記録データに埋め込んで記録し、再生時には、不揮発性メモリ14に登録されたユーザIDと、ディスク30から読み出されたデータから検出されたユーザIDとを比較して、両者が一致したときに、正常な再生出力を行うようにしたことにより、個人的な利用形態に限って複製を可能にする

ことができる。

【0095】また、上述の実施の形態では、記録時には、ユーザIDモジュール20を、データ記録再生装置10に接続した状態ではないと記録を実行することができないようにしたので、この点でも、ユーザの個人使用の範囲内での制限をすることができる。

【0096】そして、この実施の形態では、記録側に上記のような制限を加えた代わりに、再生側においては、不揮発性メモリ14に登録されたユーザIDと、ディスク30から読み出されたデータから検出されたユーザIDとを比較して、両者が一致しているかどうかを判別するようにしており、記録時のように、ユーザIDモジュール20を接続する必要はなく、再生時におけるユーザの使い勝手が良くなるという効果がある。

【0097】例えば、「個人使用の範囲でコピーは自由」ということを具現化する方法として、個人で取得済みの聴取権情報（例えば、その個人が持っているコンテンツのすべての情報）を自分専用のICカードに記録しておき、コンテンツを再生する際には、必ずそのICカードを再生装置に差し込むようにする方法が考えられる。この場合、ICカードを他人が使えない状態に保つために、一人一枚のICカードを持つように管理される。

【0098】このようにすれば、ICカードが、その個人のすべての聴取権情報を持つので、コンテンツの複製は、全く自由にしてしまっても問題なくなるが、その代わりに、使用者は、再生装置に差し込むICカードを持ち歩かなければならなくなるという問題がある。

【0099】しかし、上述の実施の形態の場合には、再生装置には、そのICカードのようなものは不要となるので、非常に便利である。

【0100】また、上述の実施の形態では、記録データは、ユーザIDを暗号鍵とした暗号を施して記録するようにしているので、再生時には、ユーザIDが一致したときにしか、記録データの暗号化が解除できなくなり、より個人使用の範囲内での制限を確実にすることができる。

【0101】なお、ユーザIDを暗号鍵そのものとせず、記録データの暗号化の鍵を取得するための情報などのように、暗号化に関連する情報として用いても、同様の効果が得られると期待できる。

【0102】また、上述の実施の形態では、ユーザIDモジュール20からのユーザIDの情報は、暗号化してデータ記録再生装置10に送るようにしており、このため、ユーザIDの秘匿性を高めることができるという効果もある。

【0103】なお、上述の説明では、記録ルールおよび再生ルールをオーディオデータに埋め込んだので、記録ルールおよび再生ルールの情報は、オーディオデータから検出するようにするが、記録ルールおよび再生ルール

の情報が、TOCなどに記録されていた場合には、記録対象のオーディオデータに先立ち、記録ルールおよび再生ルールの情報を取得するようにすればよい。

【0104】また、オーディオデータが圧縮されてブロック化されている場合には、ブロックとブロックの間の隙間に記録ルールおよび再生ルールの情報を埋め込むようにすることもできる。その場合には、圧縮デコードのときに、記録ルールおよび再生ルールの情報を抽出することができる。

【0105】また、データ記録再生装置10が、再生と記録が同時にでき、複製記録ができるように、記録媒体を同時に複数枚装填できるようにされている場合には、再生側のディスクから記録ルールや再生ルールの情報を予めTOCや再生データから得るようにすることもできる。

【0106】なお、以上の実施の形態では、記録ルールおよび再生ルールをオーディオデータ中に必ず記録するように説明したが、予め、システムとして、ユーザIDが得られなかったとき、また、ユーザIDが不一致のときの、記録ルールおよび再生ルールを、例えば上述のルールのうちの一つに定めておくようにすれば、記録ルールおよび再生ルールをオーディオデータ中に記録する必要はなくなる。

【0107】[第2の実施の形態] この第2の実施の形態は、データ記録再生装置が、パーソナルコンピュータに搭載される場合の例である。図8は、この第2の実施の形態の場合のシステムのブロック図である。

【0108】この第2の実施の形態のシステムは、パーソナルコンピュータ50と、前述の第1の実施の形態の場合に用いたユーザIDモジュール20とにより構成される。

【0109】この実施の形態のパーソナルコンピュータ50は、ユーザIDモジュール20を接続するための端子を備えている。そして、この端子を通じて、ユーザIDモジュール20との間でやり取りする情報は、すべて暗号化されるものである。

【0110】パーソナルコンピュータ50は、第1の実施の形態のデータ記録再生装置10と同様に、記録再生エンジン51と、記録/再生装置部52と、不揮発性メモリ54とを備えると共に、システムバス59を介して、CPU53と、入力操作部55と、表示部56と、ネットワークインターフェース57と、ハードディスク装置58とが接続される。システムバス59には、記録再生エンジン51と、記録/再生装置部52も接続されている。

【0111】そして、ネットワークインターフェース57は、ネットワーク60に接続された記憶装置61に対して接続される。ここで、ネットワーク60は、ローカルエリアネットワーク(LAN)であっても良いし、インターネットであってもよい。インターネットの場合に

は、記憶装置 61 は、所定のサーバなどに設けられた記録装置とされる。

【0112】この第2の実施の形態においても、前述の第1の実施の形態と全く同様にして、ユーザIDモジュール 20 には、ユーザ名が入力登録され、その後、パーソナルコンピュータ 50 にユーザIDの登録処理が、ユーザIDモジュール 20 から、パーソナルコンピュータ 50 に対して行われて、不揮発性メモリ 54 には、ユーザIDが登録されて記憶される。

【0113】そして、この第2の実施の形態の場合には、記録メディアとしては、第1の実施の形態の場合のディスク 30 のみではなく、ハードディスク装置 58 やネットワーク 60 に接続された記憶装置 16 も用いられる。

【0114】すなわち、この第2の実施の形態の場合の記録における入力ソースと、記録媒体（記録メディア）との組み合わせを示すと、

- ①アナログ入力あるいはデジタル入力→ディスク 30
 - ②アナログ入力あるいはデジタル入力→ハードディスク装置 58
 - ③アナログ入力あるいはデジタル入力→記憶装置 61
 - ④ディスク 30→ハードディスク装置 58
 - ⑤ディスク 30→記憶装置 61
 - ⑥ハードディスク装置 58→ディスク 30
 - ⑦ハードディスク装置 58→記憶装置 61
 - ⑧記憶装置 61→ディスク 30
 - ⑨記憶装置 61→ハードディスク装置 58
- などがある。

【0115】この9通りの他にも、ネットワーク 60 上の一つの記憶装置から、他の記憶装置に転送して書き込む処理も、記録処理の一つと考えられる。以上のいずれの記録時においても、この第2の実施の形態では、前述の第1の実施の形態と同様にして、ユーザIDモジュール 20 が接続されることを条件とすると共に、そのユーザIDモジュール 20 から取得したユーザ名およびモジュールIDとを、記録データに埋め込んで記録するようにする。この場合に、第1の実施の形態と同様に、モジュールIDは、暗号化して記録するようにする。

【0116】この場合、ハードディスク装置 58 への記録の場合には、記録再生エンジンチップ 11 で記録エンコードされたデータは、記録／再生装置部 52 を経ることなく、システムバス 59 を通じてハードディスク装置 58 に送られて、ハードディスクに格納される。

【0117】また、記憶装置 61 への記録の場合には、記録再生エンジンチップ 11 で記録エンコードされたデータは、記録／再生装置部 52 を経ることなく、システムバス 59 およびネットワークインターフェース 57 を通じて記憶装置 61 に対してネットワーク 60 に送出され、記憶装置 61 に格納されるようにされる。

【0118】そして、ディスク 30、ハードディスク装

置 58、記憶装置 62 のいずれからのオーディオデータの再生時においても、前述の第1の実施の形態と全く同様に、再生データ中から検出したユーザIDと、不揮発性メモリ 54 に記憶されていたユーザIDとの照合が行われて、両者が一致したときに、オーディオデータの再生出力を可能とするようにする。

【0119】この第2の実施の形態の場合にも、上述した第1の実施の形態と同様の効果が得られると共に、ハードディスク装置 58 を用いた高速複製が、ユーザの個人使用の範囲内という制限を保持して可能となる。また、ネットワークを通じた記憶装置へのデータ転送も、一つの記録（複製）態様とすることができるが、それも、ユーザの個人使用の範囲内という制限を保持して可能となる。

【0120】〔課金処理の例について〕次に、記録ルールおよび再生ルールが課金を条件にしている場合に対応する実施の形態を説明する。図 10 は、この例の課金処理システムの一例を示すものであり、音楽コンテンツの配付、音楽コンテンツのデータの授受については、省略されている。この実施の形態のデータ記録再生装置 10 は、複製記録ができるように構成されている。つまり、あるディスクからのデータを、別のディスクに記録することが可能とされている。

【0121】この実施の形態の場合、課金処理のために、記録に際しては複製権データが、再生に際しては聴取権データが、それぞれ使用される。これら複製権データおよび聴取権データは、ICカードや、データ記録再生装置 10 に設けられるセキュアデコーダ 17 のメモリに格納される。

【0122】複製権データおよび聴取権データは、例えば複製可能な度数および再生可能な度数であり、データ記録再生装置 10 が課金対象のコンテンツを記録／再生する度に、それぞれの度数が減算される。

【0123】これら複製権データおよび聴取権データは、複製／聴取権データ管理会社の管理下で、ユーザが所有する複製／聴取権データチャージャまたは販売店に設置された複製／聴取権データ販売端末 205 によって書き替えることが可能とされている。この例では、複製／聴取権データチャージャは、ユーザIDモジュール 20 内に課金データチャージャ 25 として設けられている。

【0124】課金データチャージャ 25 は、データ記録再生装置 10 のセキュアデコーダ 17 と決済センター 203 またはレコード店、コンビニエンスストア等に設置されているデータ販売端末 205 との間に存在して聴取権データ中継器として機能する。

【0125】また、レコード会社 201、著作権管理機構 202、ユーザデバイスとしてのデータ記録再生装置 10 と関係して、代金決済のために、決済センター 203 が存在している。決済センター 203 は、認証／課金

サーバを備えている。決済センター203は、銀行、クレジットカード会社204との間で代金の決済を行なう。

【0126】図10において、破線で示すように、レコード会社201から配布される、記録再生装置10が再生する媒体（光ディスク、メモリカード等）には、音楽コンテンツが記録されている。音楽コンテンツの配信の方法は、この他、種々のものが使用できる。また、記録再生装置10は音楽コンテンツを媒体（光ディスク、メモリカード等）30に記録する。

【0127】データ記録再生装置10内のセキュアデコード17と、課金データチャージャ25とが、この例では有線の通信路を介して通信を行い、複製／聴取権データが課金データチャージャ25からセキュアデコード17内のメモリに対して転送される。複製／聴取権データは、例えばデータ記録再生装置10の、記録（複製）可能回数または記録（複製）可能時間／再生可能回数情報または再生可能時間に対応している。

【0128】また、データ記録再生装置10のセキュアデコード17から課金データチャージャ25に対して、データ記録再生装置10の複製／再生履歴情報（複製／再生ログ）が伝送される。複製ログには、複製したデータの識別子および／または複製の条件を含む。具体的には、複製した音楽コンテンツの識別子、種類、複製回数、複製時間等の情報を含んでいる。

【0129】再生ログは、復号したデジタルデータの識別子および／または復号の条件を含む。具体的には、聴取した音楽コンテンツの識別子、種類、再生回数、再生時間等の情報を含んでいる。この例では、再生時には、復号に対して課金される。

【0130】また、複製／再生ログには、ユーザ端末の所有者、ユーザデバイスとしてのデータ記録再生装置10の識別子等の課金対象者を特定するための識別子が含まれている。セキュアデコード17と課金データチャージャ25との間では、前述の図1に示した暗号処理部112と暗号処理および制御部21を利用して、必要に応じて認証を行い、認証が成立すると、暗号化された複製／聴取権データおよび複製／再生ログの伝送がなされる。

【0131】複製／聴取権データは、決済センター203から通信路206例えば電話回線を介して課金データチャージャ25に渡される。または、決済センター203から通信路207を介して販売端末205に渡された複製／聴取権データが通信路208を介して課金データチャージャ25に渡される。この場合にも、セキュリティの確保のために、認証と暗号化とがなされる。

【0132】課金データチャージャ25に吸い上げられた複製／再生ログは、通信路206を介して決済センター203に送られる。または、通信路208を介して販売端末205に渡される。販売端末205は、通信路2

07を介して決済センター203から聴取権データを受け取ると共に、再生ログを決済センター203へ送る。さらに、入手した聴取権データの代金を決済センター203に支払う。通信路207は、電話回線、インターネット等である。

【0133】決済センター203と聴取権データチャージャ25との間では、通信路206を介して複製／聴取権データおよび複製／再生ログの送受信がなされる。この場合にも、セキュリティの確保のために、認証と暗号化とがなされる。聴取権データの決済に関して、銀行、クレジットカード会社204が存在している。銀行、クレジットカード会社204は、予め登録してあるユーザの銀行口座から決済センター203の依頼に基づいて、課金データチャージャ25に書き込んだ複製／聴取権データ相当する金額を引き落とす。

【0134】さらに、決済センター203は、レコード会社201から複製／聴取権データに関するサービスの管理の委託を受ける。また、決済センター203は、レコード会社201に対して複製／聴取権データに関する技術の提供を行い、さらに、楽曲聴取料を支払う。レコード会社201は、著作権管理機構202に対して著作権の登録を行うことによって、著作権の管理を依頼し、著作権管理機構202から著作権料を受け取る。

【0135】なお、通信路208の代わりに、ICカードを利用することもできる。すなわち、課金データチャージャ25および販売端末205は、ICカードの書き込み／読み出し部を備えるようにする。そして、ICカードを課金データチャージャ25に差し込んだ時には、課金データチャージャ25は、ICカードに格納されている複製／聴取権データを吸い上げるとともに、複製／再生ログのデータをICカードに書き込むようにする。ICカードの複製／聴取権データは、課金データチャージャ25に吸い上げられると、クリアされて零となる。

【0136】また、販売端末205にICカードを差し込んだ時には、ユーザが必要な複製／聴取権データの度数を設定することにより、当該設定された複製／聴取権データがICカードに書き込まれる。このとき、同時に、ICカードに格納されていた複製／再生ログが販売端末205に吸い上げられ、ICカードの複製／再生ログは、クリアされる。

【0137】以上説明したような課金システムにおいて、この実施の形態では、記録ルールまたは再生ルールとして、課金処理が必要な処理が設定されていた場合には、データ記録再生装置10のセキュアデコード17において、複製または再生についての課金処理が実行される。

【0138】図11は、複製記録の際のステップS48において、記録ルールが課金を伴う記録と設定されている場合におけるステップS49での処理のフローチャートである。

【0139】すなわち、先ず、セキュアデコード17のメモリの複製権データの度数の残を調べ、課金処理可能であるか否か判別する(ステップS81)。課金処理が可能であると判別されたときには、記録(複製)を実行する(ステップS82)。そして、記録が終了したことを確認すると(ステップS83)、セキュアデコード17のメモリの複製権データの度数を減じる(ステップS84)。そして、複製ログとして、例えば複製した音楽コンテンツの識別子、種類、複製回数、複製時間等の情報をそのメモリに記憶する(ステップS85)。そして、課金処理を終了する。

【0140】一方、セキュアデコード17のメモリの複製権データの度数の残が無く、課金処理が不可の場合には、複製権データの度数残が無い旨のメッセージを出し、ユーザに知らせる(ステップS86)。そして、複製権データが追加されたか否か判別し(ステップS87)、追加されたときには、ステップS82に進み、記録を実行して、上述のステップS83以降の処理を行なう。また、複製権データの追加が無かったときには、記録不可として(ステップS88)、この課金処理ルーチンを終了する。

【0141】また、図12は、再生の際のステップS73において、再生ルールが課金を伴う再生と設定されている場合におけるステップS74での処理のフローチャートである。

【0142】すなわち、先ず、セキュアデコード17のメモリの聴取権データの度数の残を調べ、課金処理可能であるか否か判別する(ステップS91)。課金処理が可能であると判別されたときには、再生データの暗号を解除する復号を実行する(ステップS92)。そして、復号が完了したことを確認すると(ステップS93)、セキュアデコード17のメモリの聴取権データの度数を減じる(ステップS94)。そして、再生ログとして、例えば再生した音楽コンテンツの識別子、種類、再生回数、再生時間等の情報をそのメモリに記憶する(ステップS95)。そして、課金処理を終了する。

【0143】一方、セキュアデコード17のメモリの聴取権データの度数の残が無く、課金処理が不可の場合には、聴取権データの度数残が無い旨のメッセージを出し、ユーザに知らせる(ステップS96)。そして、聴取権データが追加されたか否か判別し(ステップS97)、追加されたときには、ステップS92に進み、復号を実行して、上述のステップS93以降の処理を行なう。また、聴取権データの追加が無かったときには、再生不可として(ステップS98)、この課金処理ルーチンを終了する。

【0144】なお、ステップS98では、完全に再生不可とするのではなく、さわりの部分やさびの部分のみの再生を可とするようにしてもよい。

【0145】〔その他の実施の形態〕上述の実施の形態

においては、再生時には、ユーザIDモジュールは、データ記録再生装置あるいはパーソナルコンピュータには接続しなくても再生可能としたが、再生時にも、ユーザIDモジュールを接続しなければ、再生できないような仕組みとしてもよい。すなわち、不揮発性メモリ14を設けずに、再生時にもユーザIDモジュールの接続を必須として、ユーザIDモジュールからのユーザIDと、再生データから検出したユーザIDとを照合するようにしても良い。

【0146】また、再生処理としては、上述の実施の形態と同様とするも、例えば、再生前に、データ記録再生装置に対するユーザIDモジュールの接続を確認し、不揮発性メモリ14に記憶されているユーザIDと、使用者を示すユーザIDモジュールからのユーザIDとの照合を行って、使用者を確認してから、上述の再生動作を行うようにすることもできる。

【0147】また、上述の実施の形態の場合においては、記録時には、ユーザIDモジュールの認証確認が行うが、ユーザIDを用いた確認は行っていない。しかし、記録時に、ユーザIDモジュールをデータ記録再生装置に接続したときに、ユーザIDを用いたユーザIDモジュールの認証確認を行うようにしてもよい。

【0148】また、上述の実施の形態は、記録再生装置の場合であるが、記録専用装置や、再生専用装置にも、この発明は適用可能である。その場合、ユーザIDモジュールは、上述の第1および第2の実施の形態と同様の形態では、記録専用装置に付属すべきものである。再生専用装置の場合には、再生専用装置には、ユーザIDを、その不揮発性メモリに一旦登録すれば、再生時には、再生装置にユーザIDモジュールを接続しておく必要はない。

【0149】もつとも、これらの実施の形態にも、上述のその他の実施の形態を適用することも、勿論できる。

【0150】なお、上述の第1および第2の実施の形態におけるユーザID登録は、データ記録再生装置のうちの再生装置部分に対するユーザ登録である。前述の第1および第2の実施の形態では、記録装置に対しては、ユーザIDモジュールを必ず接続して、そのユーザIDを記録するようにするので、記録装置部分のみを考えた場合には、ユーザIDを登録する必要はない。

【0151】しかし、記録専用装置や記録再生装置の記録装置部分の機能を特定の使用者専用とする場合には、ユーザIDモジュールを用いて、ユーザIDを登録して不揮発性メモリに記憶しておき、記録の際にユーザIDが一致したときに、記録が可能となるようにする仕組みとすることもできる。

【0152】また、上述の実施の形態では、ユーザIDとしては、ユーザ名やモジュールIDを用いるようにしたが、使用者の指紋や声紋、あるいは脈などの各個人に固有の生体情報を使用するようにしても良い。その場合

に、再生装置では、不揮発性メモリに記憶されている生体情報のユーザIDと再生データから検出した生体情報のユーザIDとを照合するようにしても良いが、不揮発性メモリを設けずに、再生データから検出した生体情報のユーザIDと、指紋や声紋、あるいは脈などの生体情報入力手段から入力された生体情報のユーザIDとを照合するようにすることもできる。この場合に、生体情報入力手段は、ユーザIDモジュールを用いることができる。

【0153】なお、音楽会社などから提供される読み出し専用形式のディスクのように、市販される記録媒体は、「オリジナル」として扱うこととし、前述したように、所有者は無しとされる。ただし、この「オリジナル」から複製が行なわれた場合には、その複製には、前述したように、ユーザIDが記録され、所有者が特定されることになる。

【0154】また、上述の実施の形態では、ユーザ名については、特に制限を付けなかったが、ユーザ名は個人名であっても、ファミリー名のようなグループ名であっても良い。要するに、著作権法上「個人の使用の範囲内」と認められるような範囲で共有が可能である。

【0155】また、1台の記録ないし再生装置に、複数のユーザIDを登録することができるようにして、前記1台の装置を、前記複数のユーザIDに対応する複数の使用者で共有するようにすることもできる。

【0156】また、上述の実施の形態では、ユーザIDは、記録データに埋め込むようにしたが、記録データとは別領域に記録するようにしても勿論よい。また、記録データを、コンピュータデータのようにファイル単位に取り扱う場合には、ファイル単位にユーザIDを記録データに付加することができる。

【0157】また、上述の実施の形態では、記録時には、ユーザIDモジュール20をデータ記録再生装置10に接続することを必須としたが、記録時に、ユーザIDモジュール20を接続することなく、データ記録再生装置10の不揮発性メモリ14に蓄えられているユーザID（特にモジュールID）と、記録対象のデータに付随するユーザIDとを比較照合するようにしてもよい。

【0158】また、記録ルールとして、不揮発性メモリ14に記憶されているユーザIDと、記録対象のデータに付随するユーザIDとが一致したときには、ユーザIDモジュール20はデータ記録再生装置10には接続不要という設定を行なえるようにしてもよい。

【0159】また、記録対象のデータに付随するユーザIDというときには、記録対象のデータに埋め込まれていることのみを意味するのではなく、上述したように、記録媒体のTOCエリアや、その他の記録対象データの記録部分とは別個のエリアから、ユーザIDを取得することも含む。また、インターネットからダウンロードしたデータを記録対象とする場合に、そのダウンロー

ドデータの最初、中間あるいは最後に、ユーザIDが付加されるような場合も含む。

【0160】記録対象のデータは、データ記録再生装置10において記録媒体から再生されたものではなく、アナログ入力とされた、あるいはデジタル入力とされたデータを含むものであることは言うまでもない。その場合に、その入力データは、ディスクから再生された再生データである必要もない。

【0161】なお、上述の実施の形態は、記録対象のコンテンツとして、オーディオデータを例にとったが、映像データやプログラム、ゲームのプログラムやデータなど、著作権管理が必要なコンテンツのいずれも、この発明の記録対象である。

【0162】また、記録媒体としては、ディスクに限らず、カード形メモリや、半導体メモリ、ハードディスク装置のハードディスクなどであってもよい。さらに、記録対象となるデータは、前述もしたように、記録媒体から再生されたデータに限られるのではなく、有線電話回線や無線電話回線またはインターネットを通じて送られてくるデータであってもよい。

【0163】また、上述の実施の形態は、記録対象のコンテンツとして、オーディオデータを例にとったが、映像データやプログラム、ゲームのプログラムやデータなど、著作権管理が必要なコンテンツのいずれも、この発明の記録対象である。

【0164】また、上述の実施の形態では、ユーザIDは、記録データに埋め込むようにしたが、記録データとは別領域に記録するようにしても勿論よい。また、記録データを、コンピュータデータのようにファイル単位に取り扱う場合には、ファイル単位にユーザIDを記録データに付加することができる。

【0165】

【発明の効果】以上説明したように、この発明によれば、記録時に、登録されたユーザIDを記録データと共に記録し、再生時には、不揮発性メモリ14などに用意されるユーザIDと、記録媒体から読み出されたデータから検出されたユーザIDとを比較して、両者が一致したときに、正常な再生出力を行うようにしたことにより、個人的な利用形態に限って複製を可能にすることができる。

【図面の簡単な説明】

【図1】この発明の第1の実施の形態を示すブロック図である。

【図2】この発明の第1の実施の形態の動作説明のためのフローチャートである。

【図3】この発明の第1の実施の形態の動作説明のためのフローチャートである。

【図4】この発明の第1の実施の形態の動作説明のためのフローチャートである。

【図5】この発明の第1の実施の形態における記録処理

の説明のためのフローチャートの一部である。

【図6】この発明の第1の実施の形態における記録処理の説明のためのフローチャートの一部である。

【図7】この発明の第1の実施の形態における再生処理の説明のためのフローチャートの一部である。

【図8】この発明の第1の実施の形態における再生処理の説明のためのフローチャートの一部である。

【図9】この発明の第2の実施の形態のブロック図である。

【図10】この発明の実施の形態における課金処理システムの全体の概要を説明するための図である。

【図11】この発明の実施の形態における記録時（複製時）の課金処理を説明するためのフローチャートであ *

る。

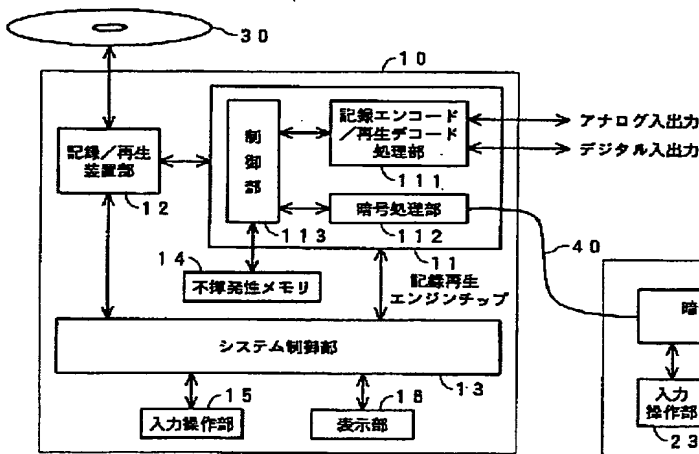
【図12】この発明の実施の形態における再生時の課金処理を説明するためのフローチャートである。

【図13】SCMS方式による複製世代制限方法を説明するための図である。

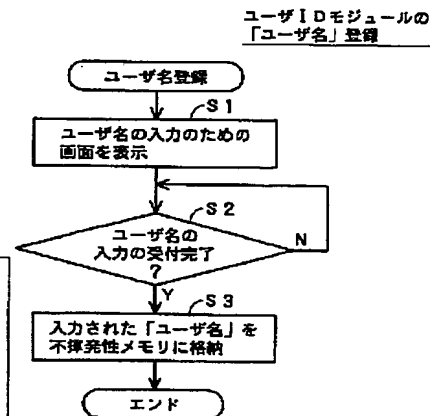
【符号の説明】

10…データ記録再生装置、11…記録再生エンジンチップ、12…記録/再生装置部、13…システム制御部、14…不揮発性メモリ、15…入力操作部、16…表示部、20…ユーザIDモジュール、21…暗号処理および制御部、22…不揮発性メモリ、23…入力操作部、24…表示部、30…ディスク、40…ケーブル、50…パーソナルコンピュータ

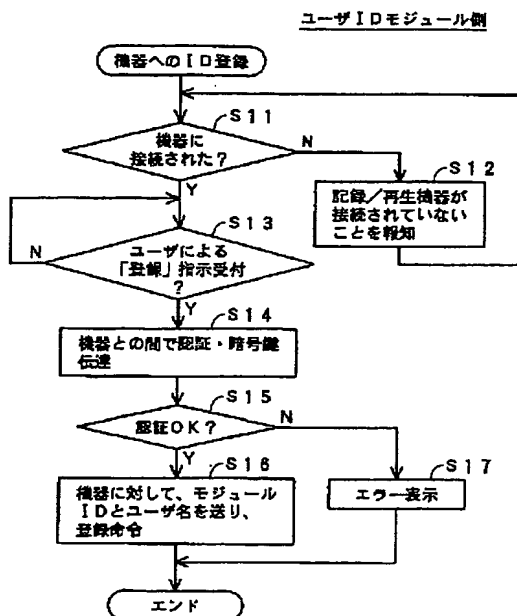
【図1】



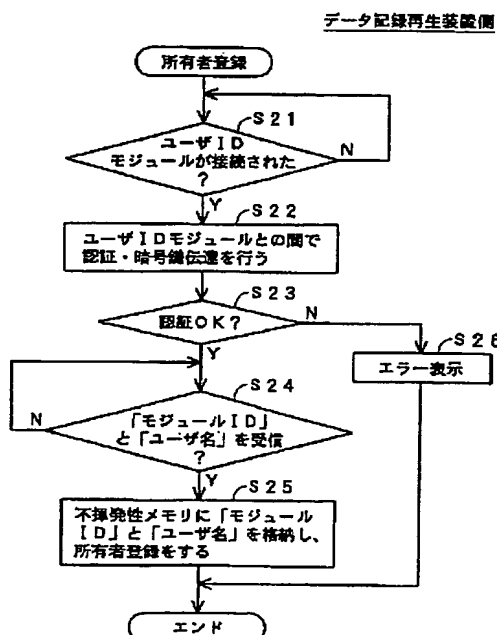
【図2】



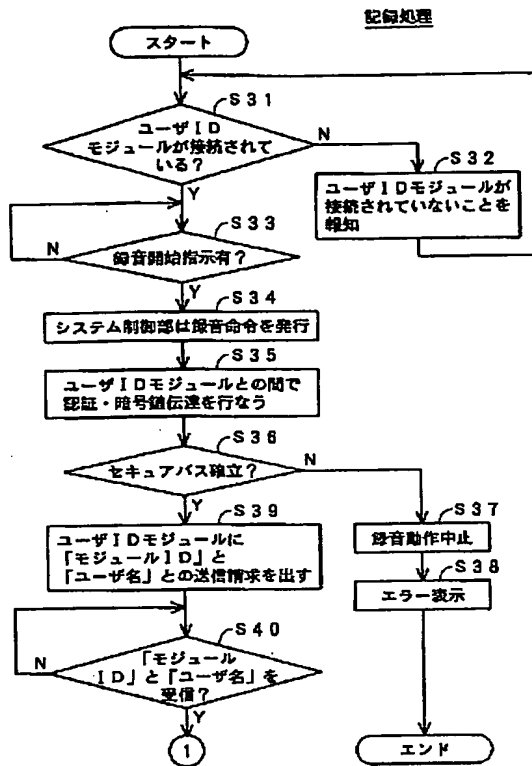
【図3】



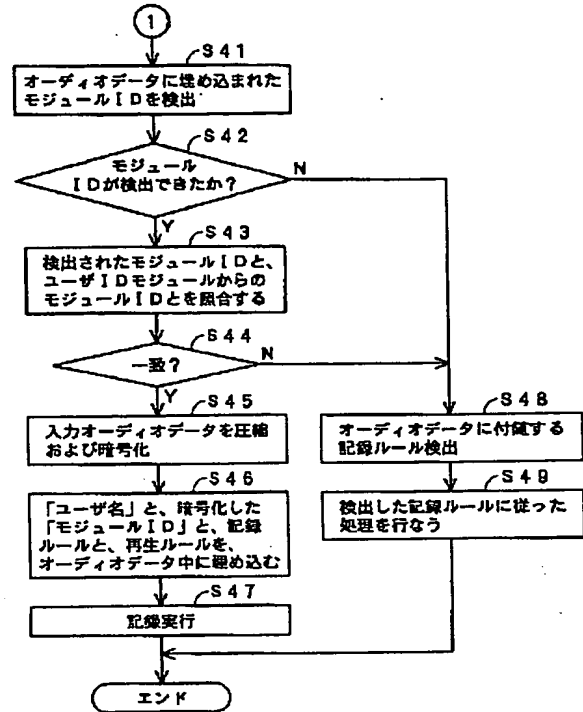
【図4】



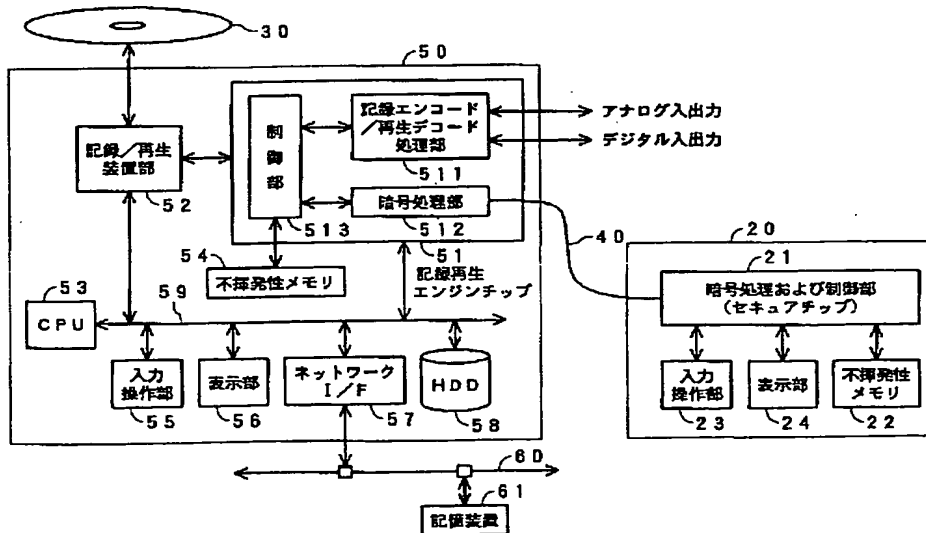
【図5】



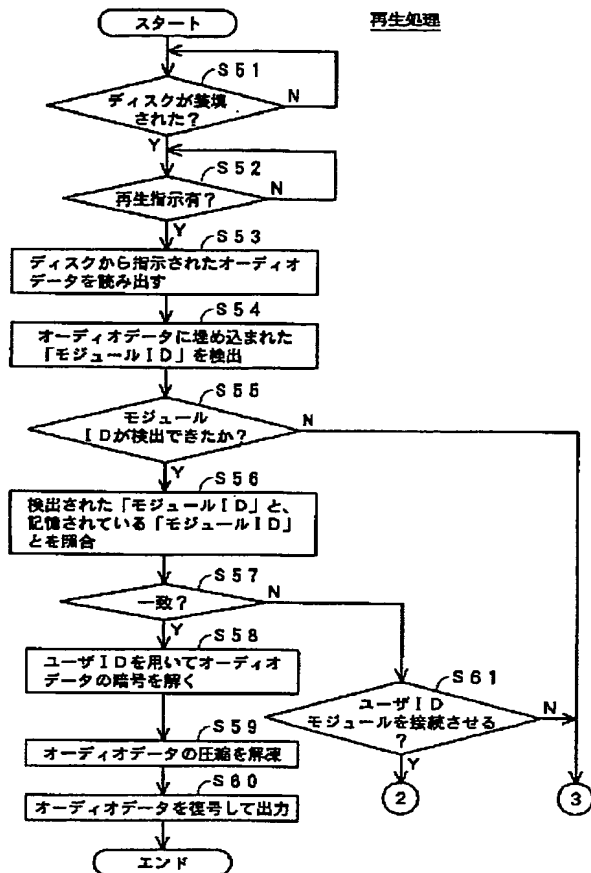
【図6】



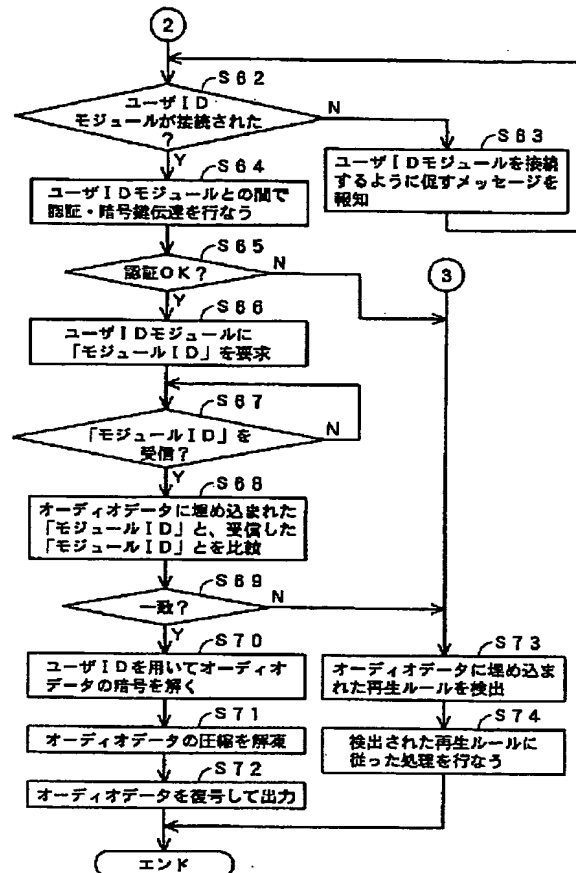
【図9】



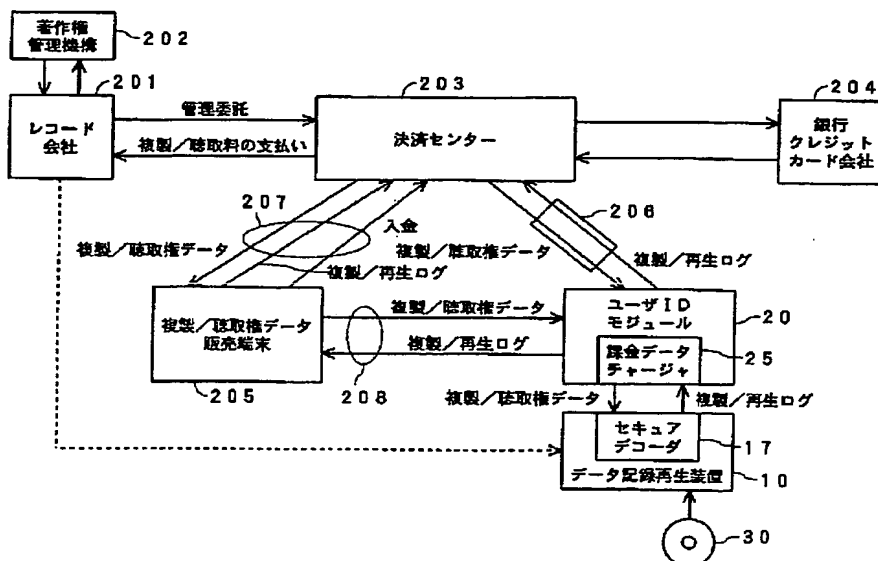
【図 7】



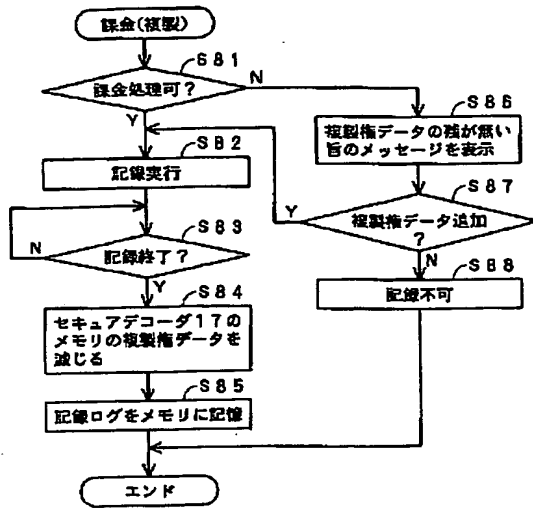
【図 8】



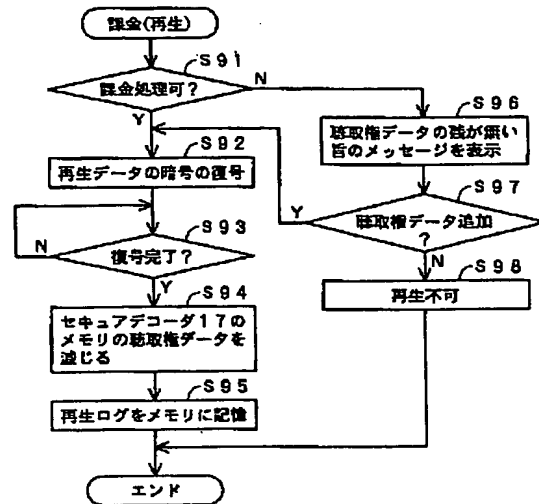
【図 10】



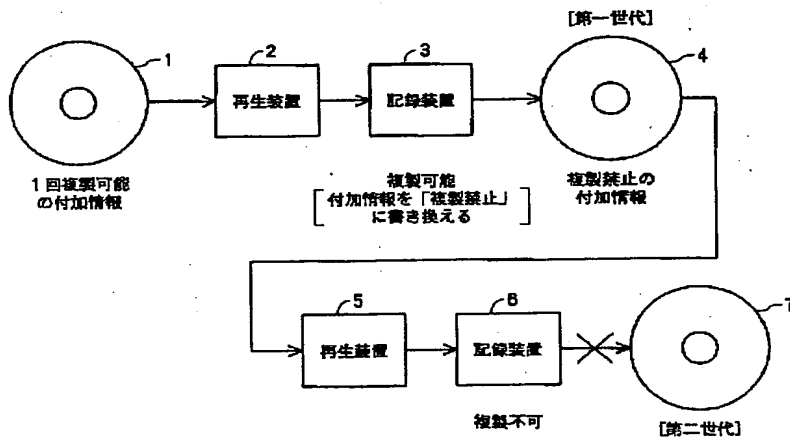
【図 11】



【図 12】



【図 13】



フロントページの続き

(72) 発明者 鳥山 充
東京都品川区北品川 6 丁目 7 番 35 号 ソニ
ー株式会社内

Fターム(参考) 5D044 AB02 AB05 AB07 BC05 BC06
CC06 DE50 DE54 EF05 FG18
GK12 GK17 HL02 HL08 HL11
5J104 AA07 AA13 AA14 EA04 EA26
KA01 KA15 KA16 KA17 KA18
MA01 NA01 NA02 NA27 NA36
NA37 NA39 NA41 PA11

THIS PAGE BLANK (USPTO)

(19)



Europäisches Patentamt
European Patent Office
Office européen des brevets



(11)

EP 1 302 944 A1

(12)

EUROPEAN PATENT APPLICATION

published in accordance with Art. 158(3) EPC

(43) Date of publication:
16.04.2003 Bulletin 2003/16

(21) Application number: 01948047.4

(22) Date of filing: 17.07.2001

(51) Int Cl.7: **G11B 20/10**

(86) International application number:
PCT/JP01/06183

(87) International publication number:
WO 02/007161 (24.01.2002 Gazette 2002/04)

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU
MC NL PT SE TR

(30) Priority: 17.07.2000 JP 2000216388
30.08.2000 JP 2000260467

(71) Applicant: Sony Corporation
Tokyo 141-0001 (JP)

(72) Inventors:
• INOKUCHI, Tatsuya, c/o SONY CORPORATION
Tokyo 141-0001 (JP)

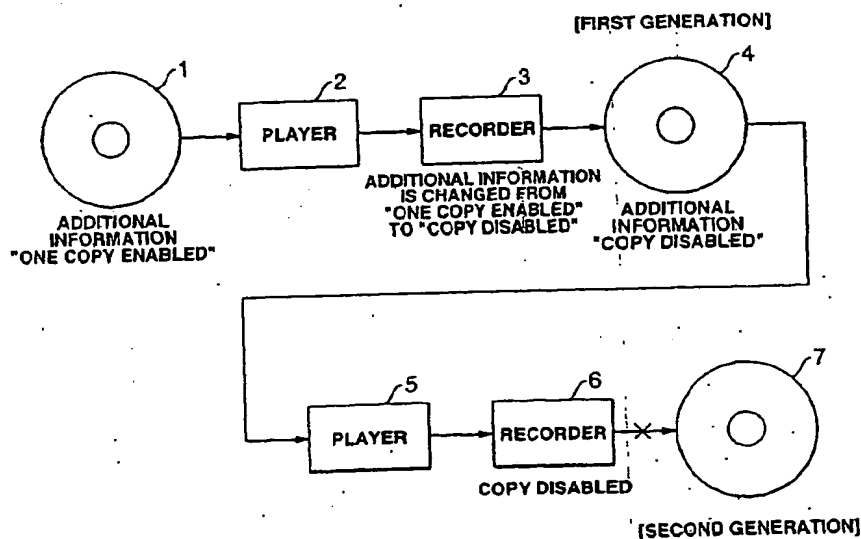
• SAKO, Yoichiro, c/o SONY CORPORATION
Tokyo 141-0001 (JP)
• TORIYAMA, Mitsuru, c/o SONY CORPORATION
Tokyo 141-0001 (JP)

(74) Representative: Ayers, Martyn Lewis Stanley et al
J.A. KEMP & CO.,
14 South Square,
Gray's Inn
London WC1R 5JJ (GB)

(54) **METHOD AND APPARATUS FOR RECORDING AND/OR REPRODUCING DATA AND RECORD MEDIUM**

(57) A method of recording and/or reproducing data to and/or from a recording medium is provided. A user identification data read from a recording medium having recorded therein main data to be recorded and/or reproduced and the user identification data is compared with

a one read from a data recorder/player for recording or reproducing the main data, and the main data are recorded to or reproduced from the recording medium when the user identification data read from the recording medium is coincident with that read from the data recorder/player.

**FIG.1**

EP 1 302 944 A1

Description

Technical Field

[0001] The present invention relates to a method of and/or apparatus for recording and reproducing content data whose copyrights have to be managed, such as audio information, video information, game program and data, computer program, etc.

Background Art

[0002] As the digital contents have become prevalent, the infringement on their copyrights by illicit copying has given birth to a social problem. In analog recording to a tape medium, audio or video data are recorded in an analog manner and so copying of the data will result in a lower quality. In digital data recording or reproduction, however, a digital data recorder/player can be used to repeatedly copy audio or video data many times with no quality degradation, in principle.

[0003] Thus, the loss due to such illicit copying has become greater in the field of digital recording/reproduction than in the analog field, and thus it has become very important to prevent illicit copying with any digital recording/players.

[0004] To solve the above problem, it has been proposed to add copy-control information to digital contents and use the added information in order to prevent illicit copying of the digital contents.

[0005] For example, the copyright protection method employing a generation-limiting copy control called "SCMS (serial copy management system)" is applied to digital data recorder/players for CD (compact disc), MD (mini disc; registered trademark), DAT (digital audio tape), etc. The SCMS copy-control method is to authorize to copy an audio content once but inhibit any further copying of the thus once copied audio content.

[0006] The SCMS copy-control method will be described in detail below with reference to FIG. 1.

[0007] For example, it is assumed here that a disc 1 has original-source audio signals digitally recorded therein. The digital audio signals are recorded in a predetermined recording format in the disc 1, and there is recorded in a specific area in the digital signals additional information indicating that the SCMS copy-control method permits to copy the digital audio signals only once.

[0008] A disc player 2 plays back the disc 1 to reproduce the digital audio signals from signals read from the disc 1, and sends the digital audio signals along with the additional copy-control information to a disc recorder 3. For sending the digital audio signals to the disc recorder 3, the disc player 2 will normally take a length of time equal to the time taken for reading the signals from the disc 1 (at the same speed).

[0009] Receiving the digital audio signals, the disc recorder 3 recognizes, when the information added to the

audio signals indicates that the received digital audio signals may be copied only once, that the input digital signals can be copied. The disc recorder 3 will record the digital signals as a copy to another recordable disc 4. In this case, the disc recorder 3 rewrites the additional information from "one copy allowed" to "further copy inhibited". Thus, the digital signals as the copy and also the additional information "further copy inhibited" are recorded or copied to the disc 4.

[0010] In case the digital audio signals thus recorded as the copy in the disc 4 (first-generation disc) are read from the disc 4 played in another disc player 5 and supplied to another disc recorder 6, however, since the disc recorder 6 will detect that the additional information included in the digital signals is "further copy inhibited", the digital audio signals cannot further be recorded to any recordable disc 7.

[0011] In this case, the copying speed is equal to that at which the audio signals have been sent from the disc player 2. That is, if a standard playback time is taken for reproduction of the audio signals, the copying speed will be equal to a normal playback speed.

[0012] The "standard playback time" is a real-time playback speed for audio signals, namely, it is a playback speed at which audio signals can be perceived by the person having the ordinary ability of hearing. For example, the standard speed for reproduction of data depends upon each player and is independent of the human perception.

[0013] As above, the SCMS copy-control method protects the copyright of data by permitting a first-generation copying in a recorder while inhibiting a second-generation copying from the first-generation copy.

[0014] The SCMS method is intrinsically intended to prevent copyrighted data from being copied in a large amount for unauthorized commercial distribution, rather than to inhibit such a second-generation copying. Therefore, it is not negative against the currently prevailing copyright concept that "free copying within a range of private use".

[0015] Recently, a variety of recording/reproducing media such as an MD (mini disc; registered trademark) player, card-type memory player incorporating a semiconductor memory, etc. have been commercially available. Thus, users can selectively use the MD player, card-type memory player or the like as a playing medium as they currently like. In these circumstances, copying is frequently done by the use of any of the above players, and the SCMS copy-control method allowing to copy data only from an original medium will be inconvenient even for copying of the data only for private use.

[0016] Many of the recent personal computers are provided each with a CD playing function to store (copy) musical information distributed via a CD into a hard disc in a hard disc drive built in the personal computer and reproduce the musical information from the hard disc. Copying to the card-type memory player can be effected at such a high speed that copying from the hard disc in

the personal computer will be more convenient. More precisely, copying from the hard disc to the card-type memory player provides a second-generation copy while musical information stored in the hard disc cannot be copied to the card-type memory player.

Disclosure of the Invention

[0017] Accordingly, the present invention has an object to overcome the above-mentioned drawbacks of the prior art by providing a data recording method and apparatus not adopting the SCMS copy-control method but permitting free copying within the range of private use and effective prevention of illicit copying for unauthorized commercial distribution of data.

[0018] The above object can be attained by providing a method of recording and/or reproducing data to and/or from a recording medium, including steps of:

comparing a user identification data read from a recording medium having recorded therein the user identification data along with main data, with a one read from a data recorder/player, for recording or reproduction of the main data to or from the recording medium; and
recording or reproducing the main data to or from the recording medium when the user identification data read from the recording medium is coincident with that read from the data recorder/player.

[0019] Also the above object can be attained by providing a recording-medium recorder including:

a head to scan a recording medium having stored therein a user identification data along with main data;
a memory having a user identification data recorded therein; and
a controller to compare the user identification data read by the head from the recording medium with that read from the memory and control operations for reproduction of the main data from the recording medium on the basis of the result of comparison.

[0020] Also the above object can be attained by providing a recording-medium player, including:

a head to scan a recording medium having recorded therein encrypted data as well as at least a user identification data and reproduction management data;
a memory having a user identification data stored therein; and
a controller to compare the user identification data read by the head from the recording medium with that read from the memory and control operations for playback of the recording medium on the basis of the result of comparison.

[0021] Also the above object can be attained by providing a method of controlling data copying, including steps of:

comparing a user identification data read from main data having at least the user identification data buried therein, with a one read from a data recorder/player, for copying of the main data; and
controlling data output when the user identification data extracted from the data in coincident with that read from the data recorder/player.

[0022] Also the above object can be attained by providing a data reproducing method including steps of:

comparing a user identification data extracted from main data having at least the user identification data buried therein, with a one read from a data recorder/player, for reproduction of the main data; and
reproducing the data when the user identification data extracted from the main data is coincident with that read from the data recorder/player.

[0023] These objects and other objects, features and advantages of the present invention will become more apparent from the following detailed description of the best mode for carrying out the present invention when taken in conjunction with the accompanying drawings.

Brief Description of the Drawings

[0024]

FIG. 1 explains the SCMS-based copy-generating limiting method.

FIG. 2 is a block diagram of a first embodiment of the present invention.

FIG. 3 is a flow chart for explanation of the operations of the first embodiment of the present invention.

FIG. 4 is also a flow chart for explanation of the operations of the first embodiment of the present invention.

FIG. 5 is also a flow chart for explanation of the operations of the first embodiment of the present invention.

FIG. 6 is a flow chart for explanation of the recording operations made by the first embodiment of the present invention.

FIG. 7 is a flow chart for explanation of recording operations made by the first embodiment of the present invention.

FIG. 8 is a flow chart for explanation of playback operations made by the first embodiment of the present invention.

FIG. 9 is a flow chart for explanation of playback operations made by the first embodiment of the present invention.

FIG. 10 is a block diagram of a second embodiment of the present invention.

FIG. 11 is a flow chart for general description of the entire billing system in the embodiments of the present invention.

FIG. 12 is a flow chart for explanation of a billing made for recording (copying) in the embodiments of the present invention.

FIG. 13 is a flow chart for explanation of a billing made for playback in the embodiments of the present invention.

Best Mode for Carrying Out the Invention

[0025] The present invention will be described in detail concerning recording and reproduction of audio signals to and from a disc-shaped recording medium, by way of example.

[First embodiment]

[0026] FIG. 2 is a block diagram of the first embodiment of the data recording/playback system according to the present invention.

[0027] As shown in FIG. 2, the recording/playback system includes a data recorder/player 10 according to the present invention, and a user identification image server 20. The user identification data server 20 will also be referred to as "user ID module" in the following description. According to this embodiment, all the data recorder/players 10 are provided with terminals for connection of the user ID module 20. Information transferred between the data recorder/player 10 and user ID module 20 via the interconnection terminals is encrypted for security.

[0028] As shown, the data recorder/player 10 includes a recording/playback signal processor (will be referred to as "recording/playback engine chip" hereunder) 11, recording/playback unit 12, system controller 13, nonvolatile memory 14, input controller 15, and a display unit 16. The recording/playback engine chip 11 includes, as functional units, a recording encoder/playback decoder 111, encryption unit 112 to establish a communication bus for encrypted-data communication with the user ID module 20, and a controller 113.

[0029] The recording encoder/playback decoder 111 included in the recording/playback engine chip 11 is controlled by the system controller 13 to encode, for recording, analog or digital audio signals supplied thereto and provide the thus encoded signals to the recording/playback unit 12, for recording, as will be described later, and decode, for reproduction, the data reproduced from the recording/playback unit 12 and outputting the thus decoded signals, for data reproduction, as will also be described later.

[0030] The encryption unit 112 in the recording/playback engine chip 11 is connected to the user ID module 20 by a cable 40 in the embodiment shown in FIG. 2. In

this embodiment, the encryption unit 112 functions, under the control of the system controller 13, to make mutual authentication with the user ID module 20 and establish a communication path to the user ID module 20 when they have successfully authenticated each other. In this case, to prevent any fraudulence such as a pretense as an authorized data recorder/player 10, a new encryption key for encryption and decryption is transmitted between the data recorder/player 10 and user ID module 20, and used to encrypt data to be transferred between the data recorder/player 10 and user ID module 20, before making any communication between the data recorder/player 10 and user ID module 20.

[0031] The controller 113 in the recording/playback engine chip 11 controls the recording encoder/playback decoder 111 and the encryption unit 112 according to a control signal supplied from the system controller 13, while controlling write and read of a user identification data to the nonvolatile memory 14 connected to the controller 113.

[0032] The recording/playback unit 12 is controlled by the system controller 13 to record the recorded signals from the recording/playback engine chip 11 to a disc 30, and also supplies the data read from the disc 30 to the recording/playback engine chip 11.

[0033] The system controller 13 provides a control conforming to an instruction given by the user operating the input controller 15, and sends necessary data to the display unit 16 for display on the screen of the latter. The display element of the display unit 16 may be a liquid crystal display, for example.

[0034] The user ID module 20 is accessory to one data recorder/player 10, and supplies a user identification data (will be referred to as "user ID" hereunder) to the data recorder/player 10. As shown in FIG. 2, the user ID module 20 includes an encryption/control unit (will be referred to as "security chip" hereunder) 21, nonvolatile memory 22, input controller 23 and a display unit 24.

[0035] The security unit 21 functions to make mutual authentication with the recording/playback engine chip 11 and establish a communication path to the recording/playback engine chip 11 when they have successfully authenticated each other. In this case, to prevent the aforementioned fraudulence such as a pretense, a new encryption key for encryption and decryption is transmitted between the data recorder/player 10 and user ID module 20 before making communication between the data recorder/player 10 and user ID module 20.

[0036] The nonvolatile memory 22 has module identification information unique to each user ID module 20 (will be referred to as "module ID" hereunder) such as a unique numeral value written therein at shipment from factory.

[0037] After purchasing the data recorder/player 10, the user shall operate the input controller 23 to register his or her name (user name) to the user ID module 20 accessory to his or her data recorder/player 10 while viewing the screen of the display unit 24.

[User name registration to user ID module 20]

[0038] FIG. 3 shows a flow of operations to be made for registering a "user name" to the user ID module 20.

[0039] First, the user ID module 20 displays a "user name" input screen on the display unit 24 to prompt the user to enter his name (user name) to the user ID module 20 (in step S1). When the user has entered his name by operating the input controller 23 while viewing the display on the display unit 24, the user ID module 20 will make sure that the user name has completely been entered via the input controller 23 (in step S2), and then store the thus entered "user name" into the nonvolatile memory 22. These operations are effected under the control of the security chip 21.

[0040] Note that when a registered user name check mode is selected via the input controller 23, the user name thus supplied and registered will be read from the nonvolatile memory 22 and displayed on the screen of the display unit 24, whereby the user can make sure the user name has been registered.

[0041] When the entered "user name" is correlated one-to-one with a "module ID" prestored in the nonvolatile memory 22, the module ID will substantially mean the user ID. That is to say, according to the present invention, the user ID means both the module ID and user name in one case, and only the module ID in another case.

[User ID registration to the data recorder/player]

[0042] After registering the user name to the user ID module 20, the user has to connect the user ID module 20 to the data recorder/player 10 for registration of his user ID to the data recorder/player 10.

[0043] FIGS. 4 and 5 show flows of operations effected in registering the user ID to the data recorder/player 10 by means of the user ID module 20. FIG. 4 shows a flow of operations made at the user ID module 20, while FIG. 5 shows a flow of operations made at the data recorder/player 10.

<Operations made at the user ID module 20>

[0044] As shown in FIG. 4, the user ID module 20 judges first whether it is connected to the data recorder/player 10 (in step S11). If the user ID module 20 judges in step S11 that it is not yet connected, it will inform the user, by displaying a list on the display unit 16 or otherwise, that the data recorder/player 10 is not yet connected to the user ID module 20, and prompt the user to connect the data recorder/player 10 to the user ID module 20 (in step S12).

[0045] When it is detected that the user ID module 20 is connected to the data recorder/player 10, the user ID module 20 waits for an "instruction for registration" given by the user via the input controller 23 (in step S13). When it is detected that the registration instruction has

been accepted, the user ID module 20 will authenticate and validate the recording/playback engine chip 11 of the data recorder/player 10 and transmit an encryption key (in step S14).

[0046] The user ID module 20 judges whether it has successfully made the mutual authentication with the recording/playback engine chip 11 and established a communication path (in step S15). If the user ID module 20 has failed in the authentication and in establishment of the communication path, it will exit this routine of operation with display of an error message on the display unit 24 (in step S17). When the user ID module 20 has succeeded in establishment of the communication path in step S15, it will read the module ID and user name from the nonvolatile memory 22, encrypt them and send them along with a registration instruction to the data recorder/player 10 (in step S16).

<Operations made at the data recorder/player 10>

[0047] As shown in FIG. 5, the data recorder/player 10 first waits until the user ID module 20 is connected thereto. When it judges that the user ID module 20 is connected (in step S21), the recording/playback engine chip 11 will authenticate and validate the user ID module 20 and transmit an encryption key (in step S22).

[0048] The recording/playback engine chip 11 judges whether it has successfully authenticated the user ID module 20 and established a communication path could (in step S23). If it is judged in step S23 that the data recorder/player 10 has failed in the authentication and in establishment of the communication path, it will exit this routine of operation with display of an error message on the display unit 16 (in step S26).

[0049] When the recording/playback engine chip 11 judges in step S23 that the communication could be established, it will wait for a registration instruction including "module ID" and "user name" sent from the user ID module 20 (in step S24). Upon confirmation of that reception, the recording/playback engine chip 11 will store the received module ID and user name into the nonvolatile memory 14 to register the device owner (in step S25).

[0050] Note that when a registered user name check mode is selected via the input controller 15, the user name thus supplied and registered will be read from the nonvolatile memory 14 and displayed on the screen of the display unit 16, whereby the user can make sure that the user name has been registered.

[0051] The user ID of the data recorder/player 10, thus registered once, can be re-set to another user ID by re-registering using the user ID module 20.

[Recording operations made at the data recording/player 10].

[0052] Next, operations made at the data recorder/player 10 for recording data will be described with ref-

erence to the flow charts shown in FIGS. 6 and 7.

[0053] For data recording in this embodiment, the user ID module 20 has to be connected to the data recorder/player 10. That is, the data recorder/player 10 first judges whether the user ID module 20 is connected thereto (in step S31). If it judges in step S31 that the user ID module 20 is not yet connected thereto, it will inform the user, by displaying on the display unit 16, that the user ID module 20 is not connected, and prompt to connect the user ID module 20 to the data recorder/player 10 (in step S32). In this case, the prompt to the user may be a video message or voice message like "the user ID module is not yet connected. For recording, connect the user ID module". The video message is displayed on the display unit 16.

[0054] If the data recorder/player 10 detects in step S31 that the user ID module 20 is connected thereto, it will wait for an "instruction for recording" given by the user via the input controller 15 (in step S33). When it is detected in step S33 that a "recording instruction" is received, the system controller 13 of the data recorder/player 10 supplies a recording instruction to the recording/playback engine chip 11 and recording/playback unit 12 to make preparations for data recording (in step S34).

[0055] Next, the recording/playback engine chip 11 authenticates and validates the security chip 21 in the user ID module 20, and transmits an encryption key (in step S35). The recording/playback engine chip 11 judges whether it has successfully authenticated the security chip 21 and established a communication path (in step S36). If it judges in step S36 that it has failed in the authentication of the security chip 21 and thus in establishment of a communication path, the recording/playback engine chip 11 will cease the recording procedure (in step S37) and then exit this routine of operation with display of an error message on the display unit 24 (in step S38).

[0056] When the recording/playback engine chip 11 judges in step S36 that the communication path could be established, it will issue a request for sending a user ID, that is, a module ID and user name in this case, to the user ID module 20 (in step S39).

[0057] In response to the request for sending the user ID, the security chip 21 in the user ID module 20 reads the module ID and user ID from the nonvolatile memory 22, encrypts them and sends them to the data recorder/player 10. The recording/playback engine chip 11 in the data recorder/player 10 will check if the module ID and user ID have been received by the data recorder/player 10 (in step S40).

[0058] After making sure the reception of the module ID and user ID in step S40, the recording/playback engine chip 11 tries to detect the module ID buried in audio data (in step S41), and judges whether the module ID could be detected (in step S42). If the module ID could be detected in step S42, the recording/playback engine chip 11 collates, by comparison, the detected module ID with a one available from the user ID module 20 (in step

S43).

[0059] The recording/playback engine chip 11 judges whether the collation made in step S43 shows that both the module IDs is coincident with each other (in step S44). When both the module IDs are found to be coincident with each other, the recording/playback engine chip 11 enables the recording, compresses the input audio data and encrypts them with the received user ID being taken as an encryption key (in step S45).

[0060] In this case, however, only the user name, only the module ID or both may be used as the encryption key.

[0061] There will be buried in the audio data compressed and encrypted in step S45 "user name" and "module ID" available from the user ID module 20 (in step S46). In this case, the module ID is encrypted before being buried to improve the concealment of the user ID. Further in step S46, a recording rule and reproduction rule are buried in the audio data to be recorded.

[0062] As above, the audio data in which the encrypted user ID etc. are buried are recorded to the disc 30 as a recording medium (in step S47).

[0063] On the other hand, if the module ID could not be detected in step S42 and when there is found in step S44 no coincidence between the module ID detected from the audio data and module ID available from the user ID module 20, the recording rule buried in the audio data is detected (in step S48) and operations conforming to the detected recording rule are effected (in step S49).

[0064] For burying information such as the recording rule, a technique called "digital watermarking" or any other well-known burying technique may be used. Also, such information may be buried not in audio data but in a recording area other than a recording area in which audio data are recorded such as an area where TOC (table of contents) data is recorded or in a sub code area.

[0065] The above-mentioned recording rules to be buried include the following of which any one is selected from them for burying in audio data:

- R1 Recording (copying) is allowed for free
- R2 Recording (copying) is allowed at cost
- R3 Free recording (copying)
- R4 Recording (copying) is inhibited

Contents of the recording rule themselves may be recorded as information about the recording rule or there may also be recorded information indicating which one of the above-mentioned rules R1 to R4 is to be buried.

[0066] The rule R1 "recording (copying) is allowed for free" permits to record audio data only with a user ID buried in audio data. In this embodiment, this rule is followed to record audio data to a recording medium, such as a read-only disc (will be referred to as "ROM type" disc hereunder) made by a recording company using an authoring apparatus, without any user ID being buried

since the disc is not yet owned by anybody at this stage. So, this rule is applied when recording (copying) audio data from a ROM-type recording medium.

[0067] The above rule R2 "recording (copying) is allowed at cost" permits a recorder capable of billing to record audio data only when the billing has been made. Under this rule, a recorder not capable of the billing is inhibited from recording audio data. The billing will be described in detail later using an example.

[0068] The rule R3 "free recording (copying)" permits to record (copy) audio data with no user ID being buried in the audio data. Further, the rule R4 "recording (copying) is inhibited" permits no recording of any audio data.

[0069] As above, the recording rules are applied when there is no coincidence between user IDs as well as when no user ID can be detected from audio data to be recorded. However, one recording rule may be recorded for application when no coincidence is detected between the user IDs while another recording rule may be recorded for application when no valid user ID can be detected.

[0070] For reproducing audio data in this embodiment, a user ID buried in the audio data is collated with a one stored in the nonvolatile memory 14 as will be described in detail later. When both the IDs are found to be coincident with each other, the audio data can be reproduced. In this embodiment, when no user ID can be detected in the audio data to be reproduced or when the result of collation is that the user IDs show no coincidence between them, a reproduction rule (playback condition) specifying how the audio data are to be processed is buried in the audio data in step S46.

[0071] Information about the reproduction rule may be buried in audio data using the digital watermarking or any other well-known burying technique as in the case of the aforementioned recording rule. Also, such information may be buried not in audio data but in a recording area other than a recording area in which audio data are recorded such as an area where TOC (table of contents) data is recorded or in a sub code area.

[0072] When there is no coincidence between user IDs, any one is selected from the following for burying in the audio data:

- PB1 Reproduction is allowed for free
- PB2 Reproduction is inhibited (reproduction is disabled)
- PB3 Reproduction is allowed at cost
- PB4 Reproduction is limitatively allowed

Contents of the reproduction rule themselves may be recorded as information about the reproduction rule or there may also be recorded information indicating which one of the above-mentioned rules PB1 to PB4 is to be buried.

[0073] The rule PB1 "reproduction is allowed for free" permits to always reproduce audio data independently

of any user ID registered in the player. The rule PB2 "reproduction is inhibited (reproduction is disabled)" inhibits its audio data from being reproduced when there is no coincidence between the user ID buried in the audio data and the user ID registered in the player. In this embodiment, since audio data are recorded, with no user ID buried therein, to a recording medium such as a ROM-type disc made by a recording company by the authoring apparatus as above, the rule PB1 is recorded in the audio data for application when no valid user ID can be available from the reproduced audio data.

[0074] Also, the rule PB3 "reproduction is allowed at cost" permits a player capable of billing to reproduce audio data when the billing is possible. If the player is not capable of such billing, audio data cannot be reproduced. Note that the billing will be described in detail later taking an example.

[0075] The rule PB4 "reproduction is limitatively allowed" permits to reproduce audio data for test-listening to all or a part of the audio data. After completion of the test-listening mode, the rule PB2 or PB3 is applied to the reproduction of audio data. For the test-listening, any of the following is allowed:

- (a) Free reproduction by *n* times, for example, once
- (b) Free reproduction for *m* seconds
- (c) Free reproduction of most affecting passage or climax part

[0076] When the test-listening mode (a) or (b) is applied for the reproduction rule PB4 "reproduction is limitatively allowed", information about the test-listening history of audio data identified with an ID content (identification code) such as ISRC (International Standard Recording Code), for example, number of times of test-listening, seconds for which the test-listening has been made, etc., is registered in the player correspondingly to the ID content.

[0077] In this embodiment, the reproduction rule is applied in common when no coincidence is found between the user IDs for data reproduction as well as when no valid user ID is available from reproduced audio data. However, one reproduction rule may be recorded for application when no coincidence is found between user IDs while another reproduction rule may be recorded for application when no valid user ID is available from audio data.

[0078] For example, in case a recording medium such as a ROM-type disc or the like made by a recording company using an authoring apparatus has recorded therein a specific ID like "ORIGINAL" indicating that the recording medium is an original, the player, having detected the specific ID, should be allowed to reproduce audio data from the recording medium even if the specific ID is not coincident with the user ID of the player itself. Therefore, in case a reproduction rule is to be buried in audio data, it should be "reproduction is allowed".

[0079] On the other hand, in case it is prescribed that

such a specific ID should be recorded, by burying or otherwise, in audio data recorded in a recording medium such as a ROM-type disc or the like, the audio data may be taken as illicitly recorded data if no valid user ID is available in the player. Therefore, the reproduction rule should be "reproduction is inhibited" in this case.

[0080] One of the above reproduction rules can be used in common in recording media such as ROM-type discs made by recording companies using an authoring apparatus in case it is prescribed that no user data should be recorded in the recording media.

[Reproducing operations made at the data recorder/player 10]

[0081] Next, operations made at the data recorder/player 10 for reproducing audio data having been recorded as above will be described with reference to FIGS. 8 and 9.

[0082] First, a recorded disc is loaded into the data recorder/player 10. Recognizing when the recorded disc is set in the data recorder/player 10 (in step S51), the recording/playback engine chip 11 will wait for a playback instruction from the user. When the recording/playback engine chip 11 has recognized the playback instruction given by the user via the input controller 15 (in step S52), it reads audio data which it has thus been instructed to reproduce from the disc (in step S53).

[0083] A user ID buried in the thus read audio data is detected. In this embodiment, an encrypted module ID of the user ID is decrypted to detect the user ID (in step S54). It is judged whether the module ID could be detected (in step S55). If the module ID could not be detected, a reproduction rule buried in the audio data to be reproduced is detected (in step S73) and a due step is taken according to the detected reproduction rule (in step S74).

[0084] When it is judged in step S55 that the module ID could be detected, the detected module ID is collated, by comparison, with a one stored in the nonvolatile memory 14 (in step S56).

[0085] It is judged whether the module IDs are coincident with each other (in step S57). If it is judged in step S57 that the module IDs are coincident with each other, the encrypted audio data for which the user ID is used are decrypted (in step S58), and decompressed, that is, expanded (in step S59). The expanded or decompressed audio data are decoded before being outputted (in step S60).

[0086] On the other hand, if it is judged in step S57 that there is no coincidence between the module ID detected from the audio data read from the disc 30 and that read from the nonvolatile memory 14, it is judged whether the data recorder/player 10 has been set to have the user connect the user ID module 20. If the result of judgment is that no such setting has been made, the reproduction rule buried in the audio data to be reproduced is detected (in step S73) and a due step is

taken according to the detected reproduction rule (in step S74). In this embodiment, playback of the disc 30 is inhibited, for example.

[0087] The above playback inhibition includes also blocking of the data recorder/player 10 from providing normal output of reproduced audio data. Namely, the data recorder/player 10 outputs a noise as the playback output. Alternately, the data recorder/player 10 may be adapted to provide a message like "this is a playback of an illicitly copied recording medium" instead of the playback output.

[0088] If it is judged in step S61 that the data recorder/player 10 has been set to have the user connect the user ID module 20, the data recorder/player 10 will judge whether the user ID module 20 is connected (in step S62). If it is judged in step S62 that the user ID module 20 is not connected, the data recorder/player 10 will inform the user of the fact and prompt the user to connect the user ID module 20 (in step S63).

[0089] When it is detected that the user ID module 20 is connected to the data recorder/player 10, the recording/playback engine chip 11 makes mutual authentication and validation with the user ID module 20 and transmits an encryption key (in step S64). Further the recording/playback engine chip 11 judges whether the mutual authentication and communication path establishment have successfully been made between the recording/playback engine chip 11 and user ID module 20 (in step S65). If the mutual authentication could not be made and the communication path could not be established between the recording/playback engine chip 11 and user ID module 20, the recording/playback engine chip 11 takes a due step according to the reproduction rule buried in the audio data (in steps S73 and S74). In this embodiment, playback of the disc 30 is inhibited as above.

[0090] When it is judged in step S65 that the communication path could be established between the recording/playback engine chip 11 and user ID module 20, the recording/playback engine chip 11 will send, to the user ID module 20, a request for sending a module ID in the user ID, in this embodiment (in step S66).

[0091] In response to the sending request from the recorder/playback engine chip 11, the security chip 21 in the user ID module 20 reads a module ID from the nonvolatile memory 22, encrypts it and sends the encrypted module ID to the data recorder/player 10. When the recording/playback engine chip 11 in the data recorder/player 10 validates the module ID sent from the user ID module 20 (in step S67), it will collate, by comparison, the module ID detected from the data read from the disc 30, with that received and decrypted or decoded (in step S68).

[0092] The recording/playback engine chip 11 judges whether the module IDs are coincident with each other (in step S69). When there is no coincidence between the module IDs, the recording/playback engine chip 11 will take a due step according to the reproduction rule buried in the audio data (in steps S73 and S74). As

above, playback of the disc 30 is inhibited in this embodiment.

[0093] When the module IDs are coincident with each other, the encrypted audio data are decrypted or decoded with the user ID (in step S70), decompressed or expanded (in step S71). The decompressed or expanded audio data are decoded and outputted (in step S72).

[0094] In this embodiment, data are recorded to a disc 30 with a registered user ID buried in the data, and a user ID registered in the nonvolatile memory 14 and a user ID detected from the data read from the disc 30 are compared with each other, as having been described above. When the result of comparison shows that the user IDs are coincident with each other, the data read from the disc 30 are normally reproduced and outputted. Thus, audio data can only be copied for private use.

[0095] Also in this embodiment, since the user ID module 20 is adapted to record data only when it is connected to the data recorder/player 10, audio data can only be copied for private use.

[0096] In this embodiment, the recording side is limited as above while at the playback side, a user ID registered in the nonvolatile memory 14 is compared with a user ID detected in the data read from the disc 30 to judge whether the user IDs are coincident with each other, and so for data recording, the user ID module 20 may not be connected to the data recorder/player 10. Namely, the user can reproduce the data with a greater convenience.

[0097] For "free copying only for private use", information about a personally acquired right of listening (information about all contents which it has been authorized to reproduce for private listening) may be recorded to a personal IC card which has to be inserted into the player, for reproducing the contents. This is just an example. In this case, to prevent the IC card from being used by any other user, the users are managed for each to have an exclusive IC card.

[0098] Since the IC card has recorded therein each user's right of listening for all the contents, the user can freely copy the contents. In this case, however, the user has to carry on the IC card which is to be inserted into the player each time he is going to copy the contents for listening, which will be a great inconvenience.

[0099] That is, the above embodiment is very convenient since it eliminates the above inconvenience since it requires such an IC card.

[0100] In this embodiment, since data are encrypted, for recording, with a user ID buried as an encryption key in the data, the recorded data can only be decrypted and decoded for reproduction when the user IDs are coincident with each other, which surely allows the data to be reproduced solely within a range of private use.

[0101] Note that use of a user ID not as an encryption key but as information about encryption such as information intended for acquisition of a key for encryption of data to be recorded is expectable to provide a similar effect. However, in case the recording or reproduction

rule allows data recording or reproduction even when there is no coincidence between user IDs, the user ID may not always be used as the encryption key.

[0102] In the above embodiment, information about a user ID from the user ID module 20 is encrypted and sent to the data recorder/player 10, so that the user ID can effectively be concealed.

[0103] In this embodiment, since recording and reproduction rules are buried in audio data, information about these rules is detected from the audio data. In case information about recording and reproduction rules is recorded in TOC data or TOC area, however, the information should be acquired before recording or reproducing audio data.

[0104] In case audio data have been compressed and blocked, recording and reproduction rules may be buried in a space between blocks. In this case, information about the recording and reproduction rules can be extracted for decompression and decoding of the audio data.

[0105] In case the data recorder/player 10 is designed to accommodate a plurality of recording media together for simultaneous reproduction and recording and also for data recording (copying), information about recording and reproduction rules may be acquired from TOC data or reproduced data in a disc at the reproducing side in advance.

[0106] In the aforementioned embodiment of the present invention, recording and reproduction rules have to be recorded in audio data. Note however that by designing the system so that one of the above recording and reproduction rules is always applied when no user ID is available or when there is no coincidence between user IDs, it becomes unnecessary to record the recording and reproduction rules in the audio data.

[Second embodiment]

[0107] In the second embodiment of the present invention, the data recorder/player is installed in a personal computer. FIG. 10 is a block diagram of a system to which the second embodiment is applied.

[0108] As shown, the system according to the second embodiment includes a personal computer 50 and the user ID module 20 used in the aforementioned first embodiment.

[0109] The personal computer 50 has terminals for connection of the user ID module 20. Information transferred between the personal computer 50 and user ID module 20 via the terminals for connection of the user ID module 20 is all encrypted.

[0110] Similarly to the data recorder/player 10 according to the first embodiment, the personal computer 50 includes a recording/playback engine chip 51, recording/playback unit 52 and a nonvolatile memory 54, and has connected thereto a CPU 53, input controller 55, display unit 56, network interface 57 and a hard disc drive 58 via a system bus 59. The system bus 59 has

also connected thereto the recording/playback engine chip 51 and recording/playback unit 52.

[0111] The network interface 57 is connected to a memory 61 connected to a network 60. The network 60 may be a local area network (LAN) or Internet. In case the network 60 is the Internet, the memory 61 will be a recorder provided in a predetermined server or the like.

[0112] In this second embodiment, a user name is supplied for registration to the user ID module 20 as in the aforementioned first embodiment, and further the user ID is registered from the user ID module 20 into the personal computer 50. Thus, the user ID is registered into the nonvolatile memory 54.

[0113] The second embodiment uses, as the recording medium, not only the disc 30 as in the first embodiment but the memory 61 connected to the hard disc drive 58 and network 60.

[0114] In data recording in the second embodiment, the data will flow between an input source and recording medium in combination as follows:

- (1) Analog or digital input to disc 30
- (2) Analog or digital input to hard disc drive 58
- (3) Analog or digital input to memory 61
- (4) Disc 30 to hard disc drive 58
- (5) Disc 30 to memory 61
- (6) Hard disc drive 58 to disc 30
- (7) Hard disc drive 58 to memory 61
- (8) Memory 61 to disc 30
- (9) Memory 61 to hard disc drive 58

[0115] In addition to the above nine combinations, data transfer from one memory to another in the network 60 may be considered as one of the recording operations. In each of the recording operations in the second embodiment, the user ID module 20 has to be connected to the personal computer 50 as in the first embodiment and a user name and module ID acquired from the user ID module 20 are buried in audio data. In this case, the module ID is to be encrypted as in the first embodiment.

[0116] For data recording to the hard disc drive 58 in this case, data encoded in the recording/playback engine chip 51 are sent to the hard disc drive 58 via the system bus 59, not via the recording/playback unit 52, and thus stored into the hard disc drive 58.

[0117] For data recording to the memory 61, data encoded in the recording/playback engine chip 51 are sent over the network 60 to the memory 61 via the system bus 59 and network interface 57, not via the recording/playback unit 52, and thus stored into the memory 61.

[0118] For reproduction of audio data from any of the disc 30, hard disc drive 58 and memory 62, a user ID detected in reproduced data is collated with a one stored in the nonvolatile memory 54 as in the aforementioned first embodiment. When they are coincident with each other, it is allowed to reproduce and output the audio data.

[0119] The second embodiment is as effective as the aforementioned first embodiment, and can allow a quick copying of audio data by the hard disc drive 58 solely for a private use by the user. The data transfer to the memory via the network can be considered as one manner of recording (copying) and is allowed only for the private use by the user.

[Example of billing operations]

[0120] Next, an embodiment of the present invention in which billing-based recording and reproduction rules are applied will be described with reference to FIG. 11 showing an example of billing system in which distribution and transfer of musical contents are omitted. The data recorder/player 10 included in this embodiment is adapted to record data for copying. That is, with the data recorder/player 10, data from a disc can be recorded to another disc.

[0121] For billing in this embodiment, right-of-copying data is used for recording, while right-of-listening data is used for playback. These right-of-copying and right-of-listening data are stored in an IC card or in a security decoder 17 provided in the data recorder/player 10.

[0122] The right-of-copying data and right-of-listening data are a number of times data can be copied and a number of times data can be reproduced, respectively, for example. Each time the data recorder/player 10 records or reproduces data for which the user is billed, each of the numbers is decremented.

[0123] The right-of-copying and right-of-listening data can be rewritten by a user's own right-of-copying/-listening data charger or a right-of-copying/-listening data selling terminal 205 placed at a shop under the management by a right-of-copying/listening data management company. In this embodiment, the right-of-copying/-listening data charger is provided as a billing data charger 25 in the user ID module 20.

[0124] Between the security decoder 17 of the data recorder/player 10 and the right-of-copying/-listening data selling terminal 205 placed in a settlement center 203, records shop, convenience store or the like, there is provided the billing data charger 25 which functions as a right-of-listening data relay.

[0125] The settlement center 203 is provided for settlement in relation with a recording company 201, copyright management organization 202 and data recorder/player 10 as a user device. The settlement center 203 includes an authentication/billing server, and makes a settlement in relation with a bank or credit card company 204.

[0126] In FIG. 11, a broken line indicates the distribution from the recording company 201 of a recording medium (optical disc, memory card or the like) having musical contents recorded therein and which is to be played in the data recorder/player 10. The distribution of musical contents may be done in any other different suitable manners. The data recorder/player 10 can record the

musical contents to a recording medium (optical disc, memory card or the like) 30.

[0127] In this embodiment, the security decoder 17 in the data recorder/player 10 and billing data charger 25 in the user ID module 20 communicate with each other via a cable communication path to transfer right-of-copying/-listening data from the billing data charger 25 to a memory in the security decoder 17. The right-of-copying/-listening data corresponds to a permitted number of times of recording (copying) or a permitted time length of recording (copying)/permitted number of times of reproduction or to a permitted time length of reproduction in the data recorder/player 10.

[0128] The security decoder 17 of the data recorder/player 10 sends copying/reproduction log of the data recorder/player 10 to the billing data charger 25. The copying log includes identifiers for copied data and/or copying conditions. More particularly, it includes information such as identifiers for copied contents, types of the contents, number of times of copying, copying time, etc.

[0129] The reproduction log includes identifiers for decoded digital data and/or decoding conditions. More particularly, it includes information such as identifiers for musical contents to which the user has listened, types of the contents, number of times of reproduction, reproducing time, etc. In this embodiment, billing is made to decoding for data reproduction.

[0130] The copying/reproduction log also includes identifiers to identify a billing object such as owner of the user terminal, identifier for the data recorder/player 10 as a user device, etc. Between the security decoder 17 and billing data charger 25, there is made authentication by the encryption unit 112 and encryption/control unit 21 shown in FIG. 2 when necessary. When the authentication could be made between the encryption unit 112 and encryption/control unit 21, encrypted right-of-copying/-listening data and copying/reproduction log are transmitted.

[0131] The right-of-copying/-listening data are delivered from the settlement center 203 via a communication path 206, for example, a telephone line, to the billing data charger 25. Alternatively, right-of-copying/-listening data delivered from the settlement center 203 to the right-of-copying/-listening data selling terminal 205 via a communication path 207 are delivered to the billing data charger 25 via a communication path 208. Also in this case, authentication and encryption are effected between the settlement center 203 and billing data charger 25 for example to assure the security.

[0132] The copying/reproduction log sent to the billing data charger 25 is sent to the settlement center 203 via the communication path 206. Alternatively, the copying/reproduction log is delivered to the right-of-copying/-listening data selling terminal 205 via the communication path 208. The right-of-copying/-listening data 205 receives the right of listening data from the settlement center 203 via the communication path 207 while sending the reproduction log to the settlement center 203.

Further, the right-of-copying/-listening data selling terminal 205 will pay the charge for the thus acquired right-of-listening data to the settlement center 203. The communication path 207 may be a telephone line, Internet or the like.

[0133] Between the settlement center 203 and billing data charger 25, there is transferred the right-of-copying/-listening data and copying/reproduction log via the communication path 206. Also in this case, authentication and encryption for data transfer are effected between the settlement center 203 and billing data charger 25 to assure the security. The bank and credit card company 204 are included in the system for the purpose of paying the charges for the right-of-listening data. The bank or credit card company 204 will debit a money equivalent to the right-of-copying/-listening data written to the billing data charger 25 against a pre-registered user's account upon request from the settlement center 203.

[0134] Further, the settlement center 203 is entrusted by the recording company 201 to manage the servicing of the right-of-copying/-listening data. The settlement center 203 provides right-of-copying/-listening data-related techniques to the recording company 201, and also pays for the listening to the musical data. The recording company 201 registers its copyrights in the copyright management organization 202 to request the latter for management of the copyrights and receive corresponding royalties from the copyright management organization 202.

[0135] Note that an IC card may be used instead of the communication path 208. More particularly, the billing data charger 25 and right-of-copying/-listening data selling terminal 205 are provided each with an IC card writer/reader. When the IC card is inserted into the billing data charger 25, the latter will acquire the right-of-copying/-listening data from the IC card and write the copying/reproduction log data to the IC card. When the right-of-copying/-listening data in the IC card is taken up by the billing data charger 25, it will be cleared to zero.

[0136] When a necessary number of times in the right-of-copying/-listening data is set by the user with the IC card being inserted in the right-of-copying/-listening data selling terminal 205, the set right-of-copying/-listening data will be written to the IC card. At the same time, the copying/reproduction log stored in the IC card are taken up by the right-of-copying/-listening data selling terminal 205 while the copying/reproduction log in the IC card is cleared.

[0137] In the above-mentioned embodiment of the billing system, in case an operation needing a billing is set as the recording or reproduction rule, the security decoder 17 in the data recorder/player 10 will make a billing for a data copying or reproduction.

[0138] FIG. 12 shows a flow of operations made in step S49 when the recording rule is set in step S48 for application to a billing-based copying.

[0139] First, a remaining number of times copying can

be done included in the right-of-copying data in the memory in the security decoder 17 is checked to judge whether the billing operation is possible (in step S81). When it is judged in step S81 that the billing is possible, the recording (copying) is effected (in step S82). When it is made sure that the recording is complete (in step S83), the number of times copying can be done included in the right-of-copying data in the memory of the security decoder 17 is decremented (in step S84). As copying log, information such as identifier for a copied musical content, type of the content, number of times of copying, copying time, etc. is stored into the memory (in step S85) and the billing is ended.

[0140] On the other hand, if it is judged in step S81 that no billing is possible since there remains no number of times copying can be done included in the right-of-copying data in the memory of the security decoder 17, the user is informed of the fact by displaying a message telling that there remains no number of times copying can be done in the right-of-copying data (in step S86). It is judged whether right-of-copying data has been added (in step S87). When the right-of-copying data has been added, the operation goes to step S82 where recording will be done and operations in step S83 and subsequent steps be effected. If it is judged in step S87 that there has not been added any right-of-copying data, it is judged that recording is impossible (in step S88), and the billing routine is ended.

[0141] FIG. 13 a flow of operations made in step S74 when the reproduction rule is set in step S73 to be applied to a billing-based copying.

[0142] First, a permitted number of times listening can be done included in the right-of-listening data in the memory in the security decoder 17 is checked to judge whether the billing is possible (in step S91). When it is judged in step S91 that the billing can be done, data to be reproduced are decoded for decryption (in step S92). When it is made sure that the decoding is complete (in step S93), the number of times listening can be done included in the right-of-listening data in the memory of the security decoder 17 is decremented (in step S94). As reproduction log, information such as identifier for a reproduced musical content, type of the content, number of times of reproduction, reproducing time, etc. is stored into the memory (in step S95) and the billing is ended.

[0143] On the other hand, if it is judged in step S91 that no billing is possible since there remains no number of times listening can be done in the right-of-listening data in the memory of the security decoder 17, the user is informed of the fact by displaying a message telling that there remains no number of times listening can be done in the right-of-listening data (in step S96). It is judged whether right-of-listening data has been added (in step S97). When the right-of-listening data has been added, the operation goes to step S92 where decoding will be done and operations in step S93 and subsequent steps be effected. If it is judged in step S97 that there

has not been added any right-of-listening data, it is judged that decoding is impossible (in step S98), and the billing routine is ended.

[0144] Note that the system may be adapted so that in step S98, the reproduction is not completely inhibited but reproduction of only the most affecting passage or climax part is allowed.

[Other embodiments of the present invention]

[0145] The aforementioned first and second embodiments of the present invention are adapted to reproduce data even with the user ID module not connected to the data recorder/player or personal computer. However, an embodiment other than the above may be designed to reproduce main data only when the user ID module is connected. That is, any other embodiment may be constructed with the nonvolatile memory 14 being omitted so that to collate a user ID from the user ID module with a one detected from main data to be reproduced, the user ID module has to be connected also for data reproduction.

[0146] Also, any other embodiment may be designed to operate similarly to the above first and second embodiments but only after confirming the use by making sure that the connection of the user ID module is connected to the data recorder/player and collating a user ID stored in the nonvolatile memory 14 with a one from the user ID module.

[0147] For data recording in the aforementioned first and second embodiments, the user ID module are authenticated and validated but no validation using a user ID is effected. However, when the user ID module is connected to the data recorder/player for data recording, a user ID may be used for authentication and validation of the user ID module.

[0148] The first and second embodiments concern the data recorder/player, but the present invention is also applicable to a recording-only device and playback-only device. In this case, the user ID module should be accessory to the recording-only device in any embodiments like the first and second ones. In a playback-only device, it suffices to register a user ID once in the nonvolatile memory and the user ID module has not to be kept connected to the player for data reproduction.

[0149] Of course, the above other embodiments may be modified in various manners.

[0150] Note that the registration of a user ID in the first and second embodiments is to register a user ID in a playback unit included in the data recorder/player 10. Namely, in the first and second embodiments, the user ID module should be connected to the recorder without fail to record the user ID. Therefore, in case only the recording unit is taken in consideration, it is not necessary to register any user ID.

[0151] However, in case the recording-only device or the function of the recording unit of the data recorder/player is dedicated to a specific user, a user ID may be

registered by the user ID module and stored in the non-volatile memory to permit recording only when user IDs are coincident with each other.

[0152] The above embodiments use a user name or module ID as a use ID. In addition, they may be a fingerprint or voice print of the user or biometric information unique to each individual such as pulse as the user ID. In this case, a user ID such as biometric information stored in the nonvolatile memory and a one detected from data to be reproduced may be collate with each other in the player. Alternatively, no volatile memory may be provided, and a user ID such as biometric information detected from main data to be reproduced and a one such as fingerprint, voice print or pulse, supplied from a biometric information input means may be collated with each other. In this case, the biometric information input means can use the user ID module.

[0153] Note that a commercially available recording medium such as a read-only type disc available from a recording company or the like should be handled as "ORIGINAL" and it is not owned by anyone as having previously been described. However, when data are copied from the "ORIGINAL" recording medium, a user ID will be buried in the copied data to identify the owner of the recording medium.

[0154] In the aforementioned embodiment, the user name is not specifically limited but it may be a personal name or a group name such as a family name. In short, a user name can be used in common within a range of "private use" prescribed in the Copyright Law.

[0155] By adapting a single recorder or player to register a plurality of user IDs therein, the single recorder or player can be used commonly by a plurality of users corresponding to the plurality of user IDs.

[0156] In the above embodiments, the user ID is buried in recorded. However, the user ID may of course be recorded in any area other than an area where the data are recorded. Also, when the recorded data are handled in units of file like computer data, the user ID can be added to the recorded data in units of a file.

[0157] In the above embodiments, when recording data, the user ID module 20 has to be connected to the data recorder/player 10. For data recording, however, a user ID (especially, a module ID) stored in the nonvolatile memory 14 of the data recorder/player 10 and a one carried by data to be recorded may be collated with each other by comparison without having to connect the user ID module 20 for data recording.

[0158] Also, the recording rule may be such that when the user ID stored in the nonvolatile memory 14 is coincident with a one carried by main data to be recorded, the user ID module 20 has not to be connected to the data recorder/player 10.

[0159] A user ID carried by the main data to be recorded does not only mean a one buried in the data to be recorded but also a one acquired from a TOC area of a recording medium or an area other than an area where the main data are to be recorded. Also, the user

ID includes a one added at the top, middle or end of data downloaded from the Internet.

[0160] Of course, data to be recorded includes, not ones reproduced from a recording medium in the data recorder/player 10, ones supplied as analog or digital data. In this case, the input data may not be ones reproduced from a disc.

[0161] Note that in the above embodiments, the audio data have been taken as the example of a content to be recorded but they may be any contents whose copyrights have to be managed such as video data and programs, game programs and data, etc.

[0162] The recording medium is not limited to any disc but may be a card type memory, semiconductor memory, hard disc used in a hard disc drive, etc. Further, data to be recorded are not limited to ones reproduced from a recording medium as above, but may be ones sent via a cable telephone line, radio telephone line or Internet.

20 Industrial Applicability

[0163] According to the present invention, for data recording, a registered user ID is recorded along with main data to be recorded while for data reproduction, a user ID available from the nonvolatile memory 14 is compared with a user ID detected from data read from a recording medium. When the user IDs are coincident with each other, the main data can be normally reproduced. Thus, it is permitted to copy the main data only for a private use.

Claims

1. A method of recording and/or reproducing data to a recording medium, comprising steps of:

comparing a user identification data read from a recording medium having recorded therein the user identification data along with main data, with a one read from a data recorder/player, for recording or reproduction of the main data to or from the recording medium; and recording or reproducing the main data to or from the recording medium when the user identification data read from the recording medium is coincident with a one read from the data recorder/player.

2. The method according to claim 1, wherein:

the recording medium has further recorded therein a management data to manage recording to or reproduction from the recording medium; and data are recorded to or reproduced from the recording medium based the management data read from the recording medium when the user

identification data read from the recording medium is not coincident with that read from the data recorder/player.

3. The method according to claim 1, where when the user identification data read from the recording medium is coincident with that read from the data recorder/player, main data to be recorded to the recording medium are encrypted with the user identification data read from the data recorder/player being taken as an encryption key and then recorded to the recording medium. 5
4. The method according to claim 3, wherein the user identification data read from the data recorder/player is buried in main data to be recorded to the recording medium. 10
5. The method according to claim 3, wherein the user identification data read from the data recorder/player is encrypted and buried in main data to be recorded to the recording medium. 15
6. The method according to claim 1, wherein: 20
 - the recording medium has further recorded therein a management data to manage recording to or reproduction from the recording medium; and
 - main data are reproduced from the recording medium based the management data read from the recording medium when the user identification data read from the recording medium is not coincident with that read from the data recorder/player. 25
7. The method according to claim 6, further comprising a step of permitting the data reproduction from the recording medium when the user identification data read from the recording medium is not coincident with that read from the data recorder/player and also when the user identification data read from the recording medium is a specific identification data. 30
8. The method according to claim 7, wherein the specific identification data indicates that the recording medium is an original one. 35
9. The method according to claim 1, wherein the user identification data read from the data recorder/player is set by the user. 40
10. The method according to claim 9, wherein the user identification data is a data including a user name. 45
11. A method of recording data to a recording medium, comprising steps of: 50

comparing a user identification data read from a recording medium having recorded the user identification data along with main data, with a one read from a data recorder/player, for recording the main data to the recording medium; and recording the main data to the recording medium when the user identification data read from the recording medium is coincident with a one read from the data recorder/player.

12. The method according to claim 11, wherein:

the recording medium has further recorded therein a management data to manage recording to the recording medium; and main data are recorded to the recording medium based the management data read from the recording medium when the user identification data read from the recording medium is not coincident with that read from the data recorder/player.

13. The method according to claim 11, where when the user identification data read from the recording medium is coincident with that read from the data recorder/player, main data to be recorded to the recording medium are encrypted with the user identification data read from the data recorder/player being taken as an encryption key and then recorded to the recording medium. 25
14. The method according to claim 13, wherein the user identification data read from the data recorder/player is buried in main data to be recorded to the recording medium. 30
15. The method according to claim 14, wherein the user identification data read from the data recorder/player is encrypted and buried in main data to be recorded to the recording medium. 35
16. The method according to claim 11, wherein the user-identification data read from the data recorder/player is set by the user. 40
17. The method according to claim 16, wherein the user identification data includes a user name. 45

18. A recording-medium recorder comprising:

- a head to scan a recording medium having stored therein a user identification data along with main data;
- a memory having a user identification data recorded therein; and
- a controller to compare the user identification data read by the head from the recording me-

dium with that read from the memory and control operations for playback of the recording medium on the basis of the result of comparison.

19. The apparatus according to claim 18, wherein when the user identification data read from the recording medium is coincident with that read from the memory, the controller controls the head to record main data to the recording medium.
20. The apparatus according to claim 18, wherein the memory is provided in a user identification data server connected to the data recorder/player.
21. The apparatus according to claim 20, wherein the controller makes mutual authentication with the user identification data server when it is judged that the latter is connected to the data recorder/player.
22. The apparatus according to claim 21, wherein when the authentication has successfully be made made, the controller instructs the user identification data server to read the user identification data from the memory.
23. The apparatus according to claim 22, wherein the user identification data read from the memory is encrypted and sent from the user identification data server to the controller.
24. The apparatus according to claim 21, wherein when the authentication has not successfully be made, the controller ceases the operations of recording to the recording medium.
25. The apparatus according to claim 21, wherein when it is judged that the user identification data server is not connected to the data recorder/player, the controller prompts the user to connect the user identification data server to the data recorder/player.
26. The apparatus according to claim 19, wherein:

the recording medium has further recorded therein a management data to manage recording to the recording medium; and the controller records main data to the recording medium based the management data read from the recording medium when the user identification data read from the recording medium is not coincident with that read from the memory.
27. The apparatus according to claim 26, where when the user identification data read from the recording medium is coincident with that read from the memory, main data to be recorded to the recording me-

dium are encrypted with the user identification data read from the data recorder/player being taken as an encryption key and then recorded by the head to the recording medium.

28. The apparatus according to claim 27, wherein the user identification data read from the memory is buried in main data to be recorded to the recording medium.
29. The method according to claim 28, wherein the controller encrypts the user identification data read from the memory and buries it in main data to be recorded to the recording medium.
30. The apparatus according to claim 18, wherein a user identification data set by the user is written to the memory.
31. The apparatus according to claim 18, wherein the user identification data to be stored into the memory is set by the user.
32. The apparatus according to claim 31, wherein the user identification data includes a user name.
33. A recording-medium playback method, comprising steps of:

comparing a user identification data read from a recording medium having recorded therein the user identification data along with main data, with a one read from a data recorder/player, for reproducing the main data from the recording medium; and reproducing the main data from the recording medium when the user identification data read from the recording medium is coincident with a one read from the data recorder/player.
34. The method according to claim 33, wherein:

the recording medium has further recorded therein a management data to manage the operations of data reproduction from the recording medium; and main data are reproduced from the recording medium based the management data read from the recording medium when the user identification data read from the recording medium is not coincident with that read from the data recorder/player.
35. The method according to claim 34, wherein when the user identification data read from the recording medium is not coincident with that read from the data recorder/player and also when the user identification data read from the recording medium is a

specific identification data, playback of the recording medium is allowed.

36. The method according to claim 35, wherein the specific identification data indicates that the recording medium is an original one. 5
37. The method according to claim 33, wherein:
- the recording medium has encrypted data recorded therein; and 10
- main data read from the recording medium are decrypted using, as an encryption key, the user identification data read from the recording medium when the user identification data read from the recording medium is coincident with that read from the data recorder/player. 15
38. The method according to claim 33, wherein the user identification data read from the data recorder/player is set by the user. 20
39. The method according to claim 38, wherein the user identification data includes a user name. 25
40. A recording-medium player comprising:
- a head to scan a recording medium having recorded therein encrypted data as well as at least a user identification data and reproduction management data; 30
- a memory having a user identification data stored therein; and
- a controller to compare the user identification data read by the head from the recording medium, with that read from the memory and control operations for playback of the recording medium on the basis of the result of comparison. 35
41. The apparatus according to claim 40, wherein when the user identification data read from the recording medium is coincident with that read from the memory, the controller allows to reproduce main data from the recording medium. 40
42. The apparatus according to claim 41, wherein when the user identification data read from the recording medium is coincident with that read from the memory, the controller decrypts main data read by the head from the recording medium using the user identification data. 45
43. The apparatus according to claim 42, wherein when the user identification data read by the head from the recording medium cannot be detected, the controller controls the operations for playback of the recording medium based on the reproduction man-

agement data read from the recording medium.

44. The apparatus according to claim 40, wherein the memory is provided in a user identification data server connected to the data recorder/player.
45. The apparatus according to claim 40, wherein the controller makes mutual authentication with the user identification data server when it is judged that the latter is connected to the data recorder/player.
46. The apparatus according to claim 45, wherein when the authentication has successfully be made, the controller instructs the user identification data server to read the user identification data from the memory.
47. The apparatus according to claim 46, wherein the user identification data read from the memory is encrypted and sent from the user identification data server.
48. The apparatus according to claim 45, wherein when the authentication has not successfully be made, the controller ceases the operations for data reproduction from the recording medium.
49. The apparatus according to claim 40, wherein when it is judged that the user identification data server is not connected to the data recorder/player, the controller prompts the user to connect the user identification data server to the data recorder/player.
50. The apparatus according to claim 41, wherein when the user identification data read from the recording medium is not coincident with that read from the memory and also when the user identification data read from the recording medium is a specific identification data, the controller allows to reproduce data from the recording medium.
51. The apparatus according to claim 50, wherein the specific identification data indicates the recording medium is an original one.
52. The apparatus according to claim 50, wherein the user identification data set by the user is written to the memory.
53. The apparatus according to claim 40, wherein the user identification data read from the recording medium is set by the user.
54. The apparatus according to claim 53, wherein the user identification data includes a user name.
55. A method of controlling data copying, comprising steps of:

comparing a user identification data read from main data having at least the user identification data buried therein, with a one read from a data recorder/player, for copying the main data; and controlling data output when the user identification data extracted from the data is coincident with that read from the data recorder/player.

56. The method according to claim 55, wherein:

the main data further includes a management data to manage the operations of copying the data; and
the data copying is controlled based on the management data when the user identification data extracted from the main data is not coincident with that read from the data recorder/player.

57. The method according to claim 56, wherein when the user identification data extracted from the main data is coincident with that read from the data recorder/player, the user identification data extracted from the main data is encrypted using the user identification data as an encryption key before being outputted.

58. The method according to claim 57, wherein the user identification data read from the data recorder/player is buried in the main data.

59. The method according to claim 57, wherein the user identification data read from the data recorder/player is encrypted and buried into the main data.

60. The method according to claim 56, wherein when the management data indicates that billing has to be done for copying the main data, it is judged whether the billing is possible, and the copying is done when the result of judgment is that the billing is possible.

61. The method according to claim 60, wherein the billing is such that a number of times main data can be copied is decremented.

62. The method according to claim 61, wherein when it is judged that the billing is not possible and also when the number of times main data can be copied is not incremented, the copying operation is ceased.

63. The method according to claim 55, wherein the user identification data read from the data recorder/player is set by the user.

64. The method according to claim 63, wherein the user

identification data includes a user name.

65. A data reproducing method comprising steps of:

comparing a user identification data extracted from main data having at least the user identification data buried therein, with a one read from a data recorder/player, for reproduction of the main data; and
reproducing the main data when the user identification data extracted from the main data is coincident with that read from the data recorder/player.

66. The method according to claim 65, wherein:

the main data further includes a management data to manage the operation of reproducing the main data; and
the main data are reproduced based on the management data when the user identification data extracted from the main data is not coincident with that read from the data recorder/player.

67. The method according to claim 66, wherein when the user identification data cannot be detected from the main data, the operation of reproducing the main data is controlled based on the management data.

68. The method according to claim 66, wherein when the user identification data extracted from the main data is not coincident with that read from the data recorder/player and also when the user identification data extracted from the main data is a specific identification data, it is allowed to reproduce the main data.

69. The method according to claim 68, wherein the specific identification data indicates that the recording medium is an original one.

70. The method according to claim 66, wherein when the management data indicates that billing has to be done for reproduction of the main data, it is judged whether the billing is possible, and the main data are reproduced when the result of judgment is that the billing is possible.

71. The method according to claim 70, wherein the billing is made by decrementing a number of times the reproduction can be done.

72. The method according to claim 71, wherein when it is judged that the billing is not possible and also when the number of times of reproduction is not incremented, the operation of reproduction is inhibited.

ed.

73. The method according to claim 65, wherein:

the main data includes encrypted data; and 5
the user identification data extracted from the
main data is decrypted using the user identi-
fication data when the user identification data
extracted from the main data is coincident with
that read from the data recorder/player. 10

74. The method according to claim 65, wherein the user
identification data read from the data recorder/play-
er is set by the user.

15

75. The method according to claim 74, wherein the user
identification data includes a user name.

20

25

30

35

40

45

50

55

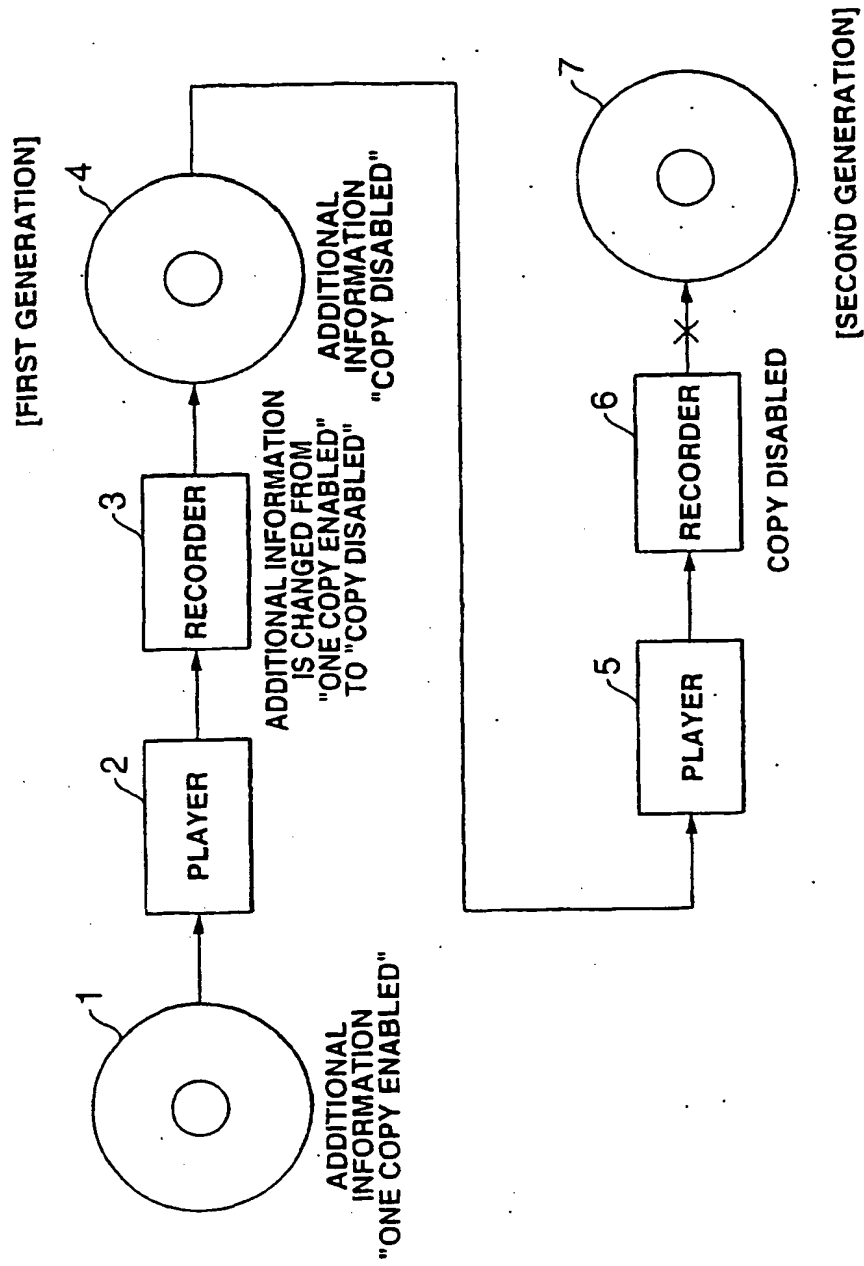


FIG.1

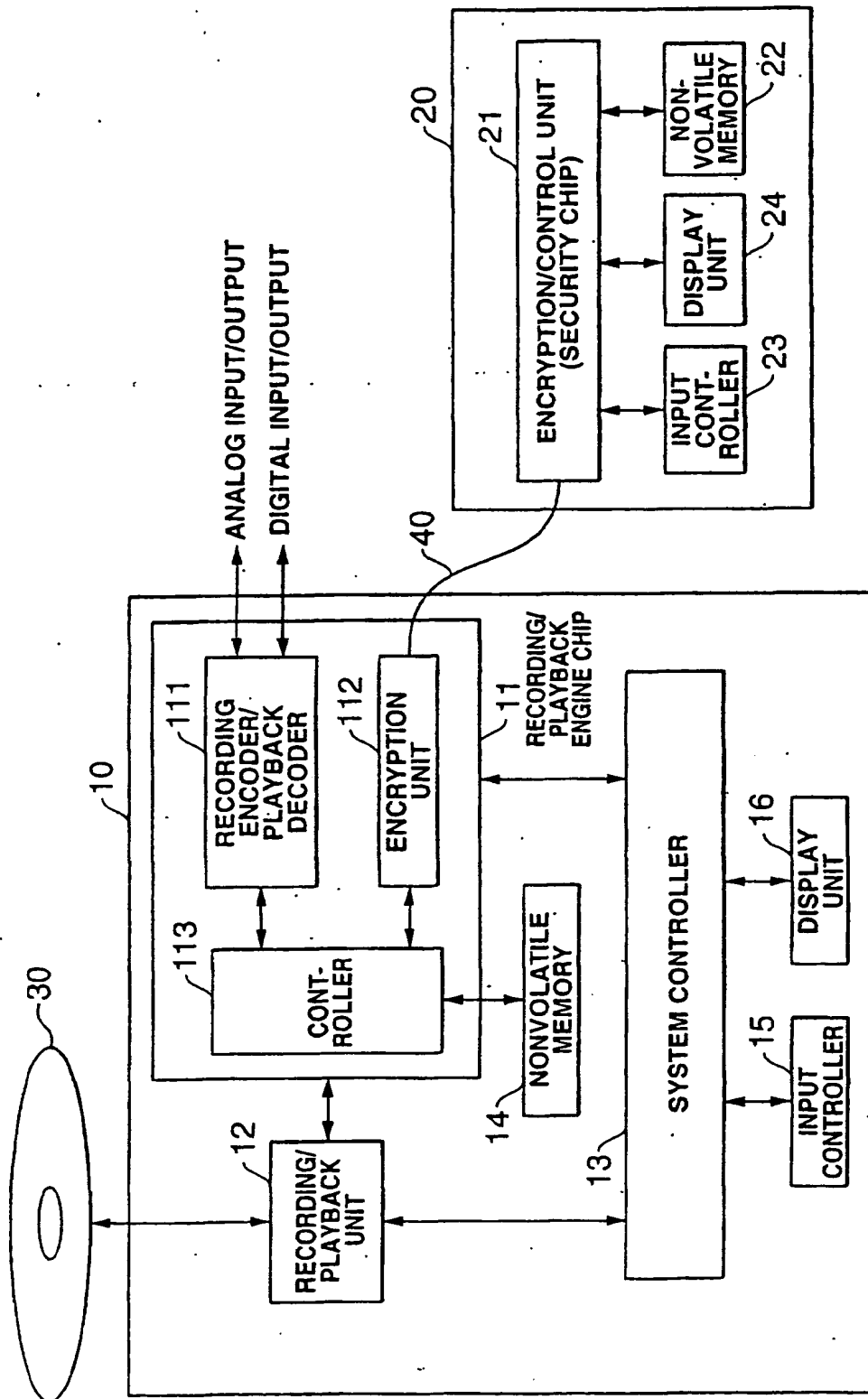


FIG.2

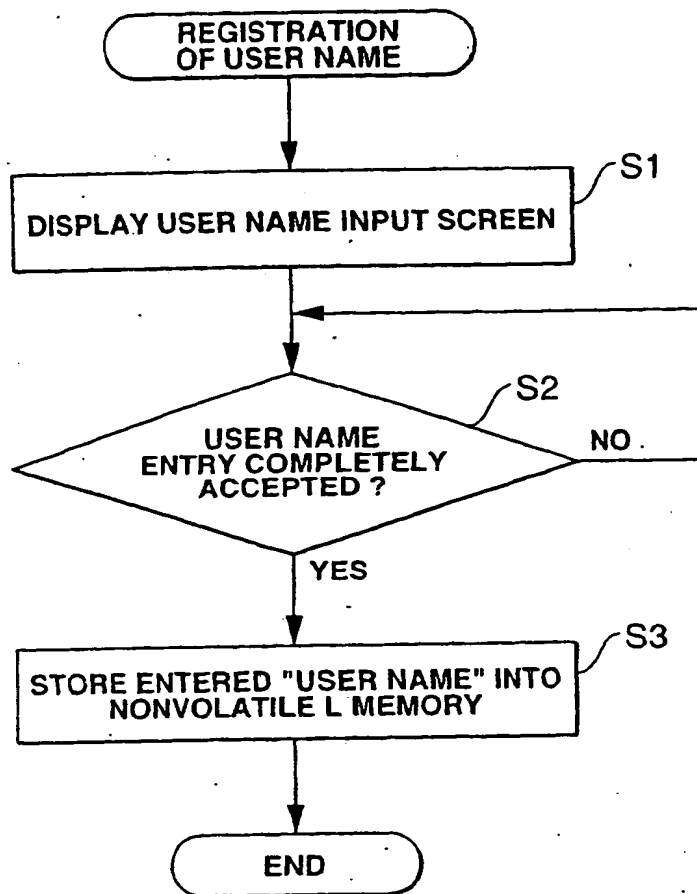


FIG.3

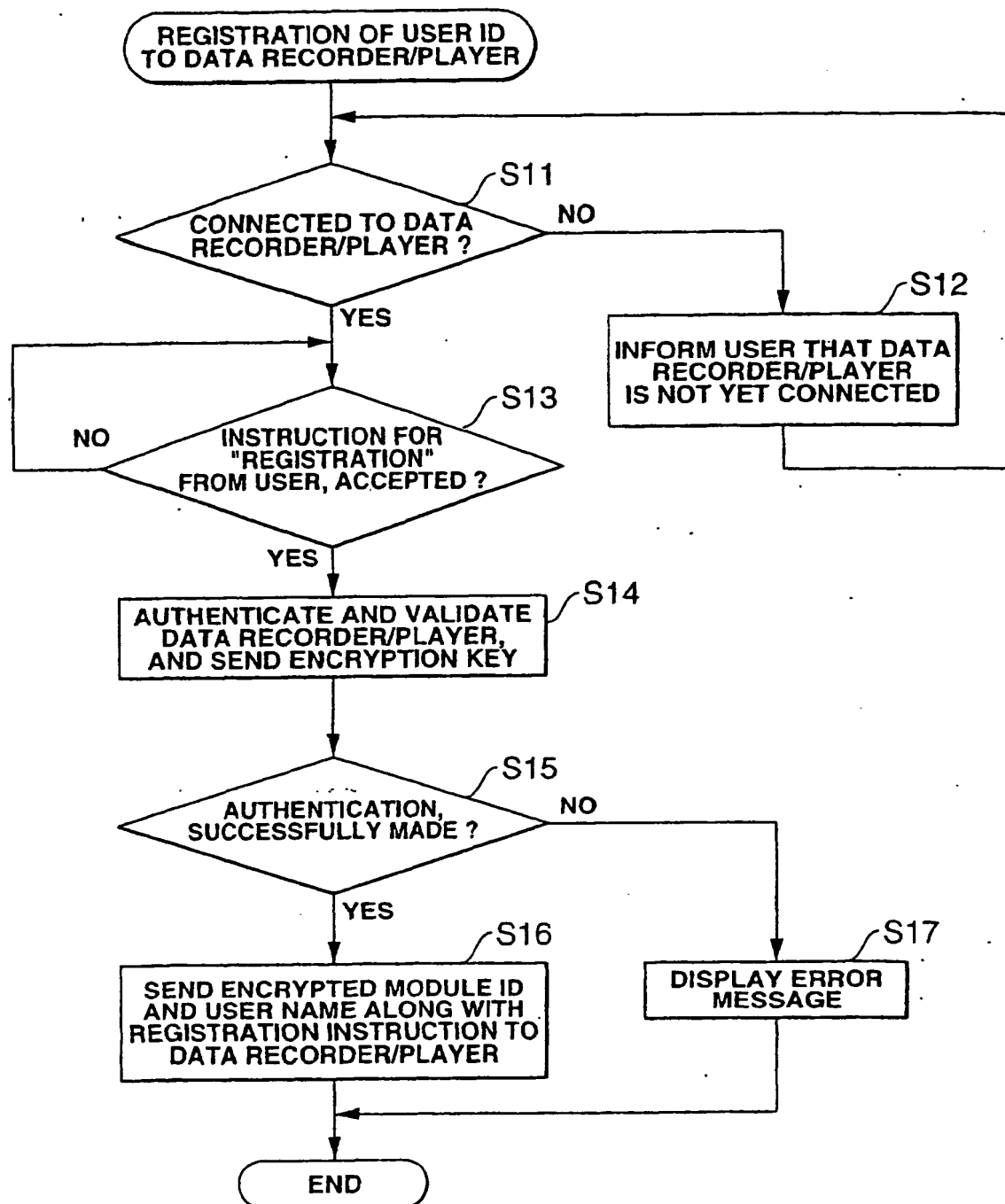


FIG.4

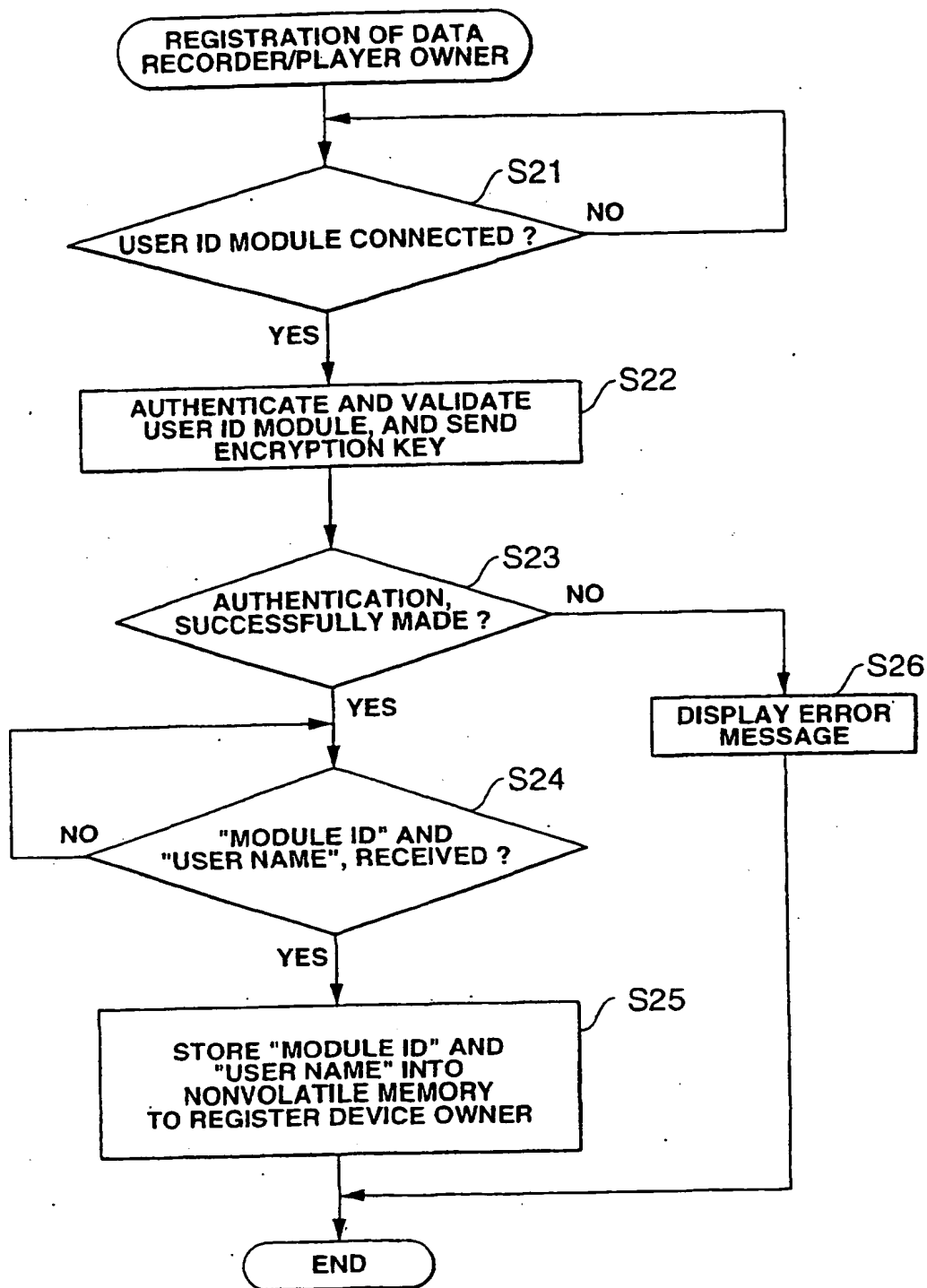


FIG.5

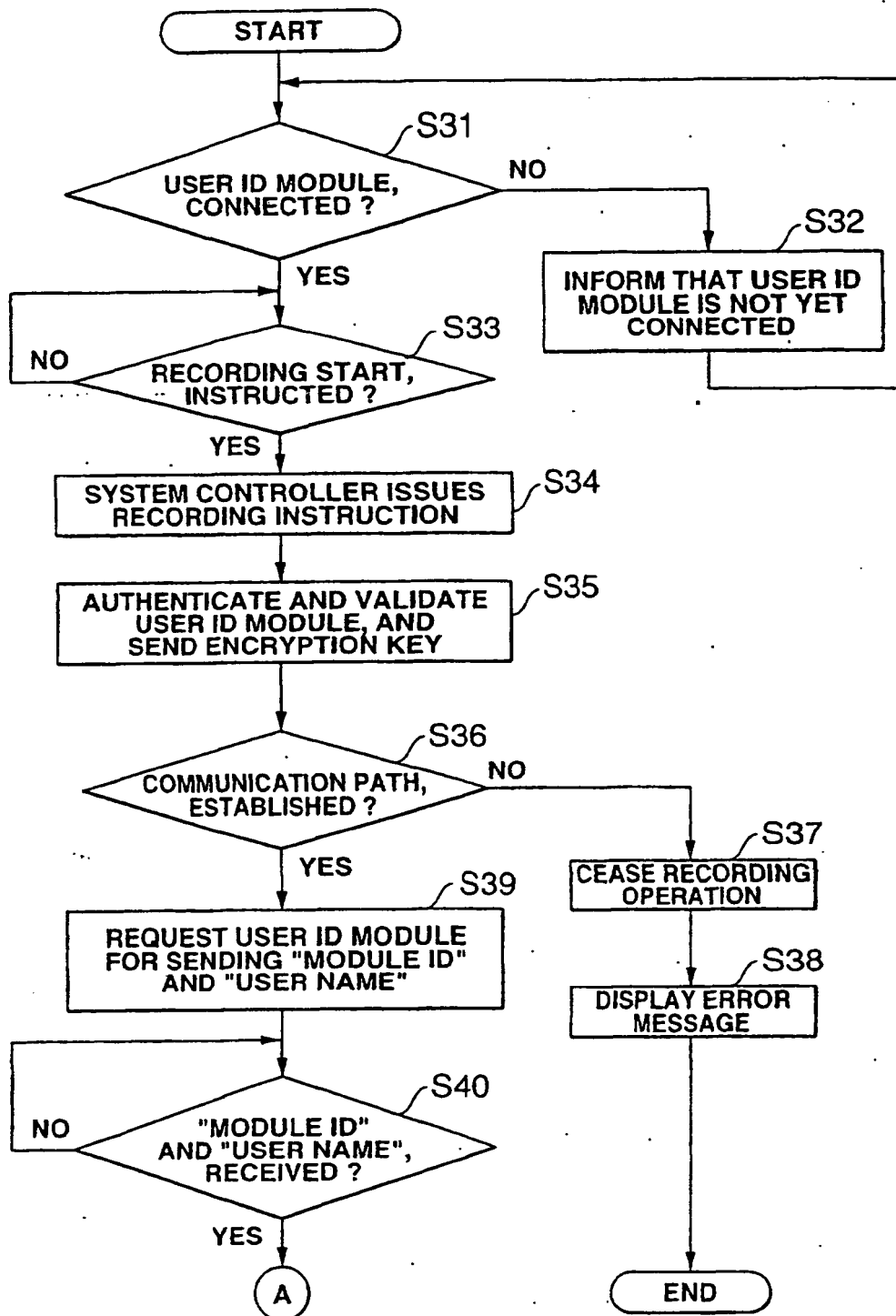


FIG.6

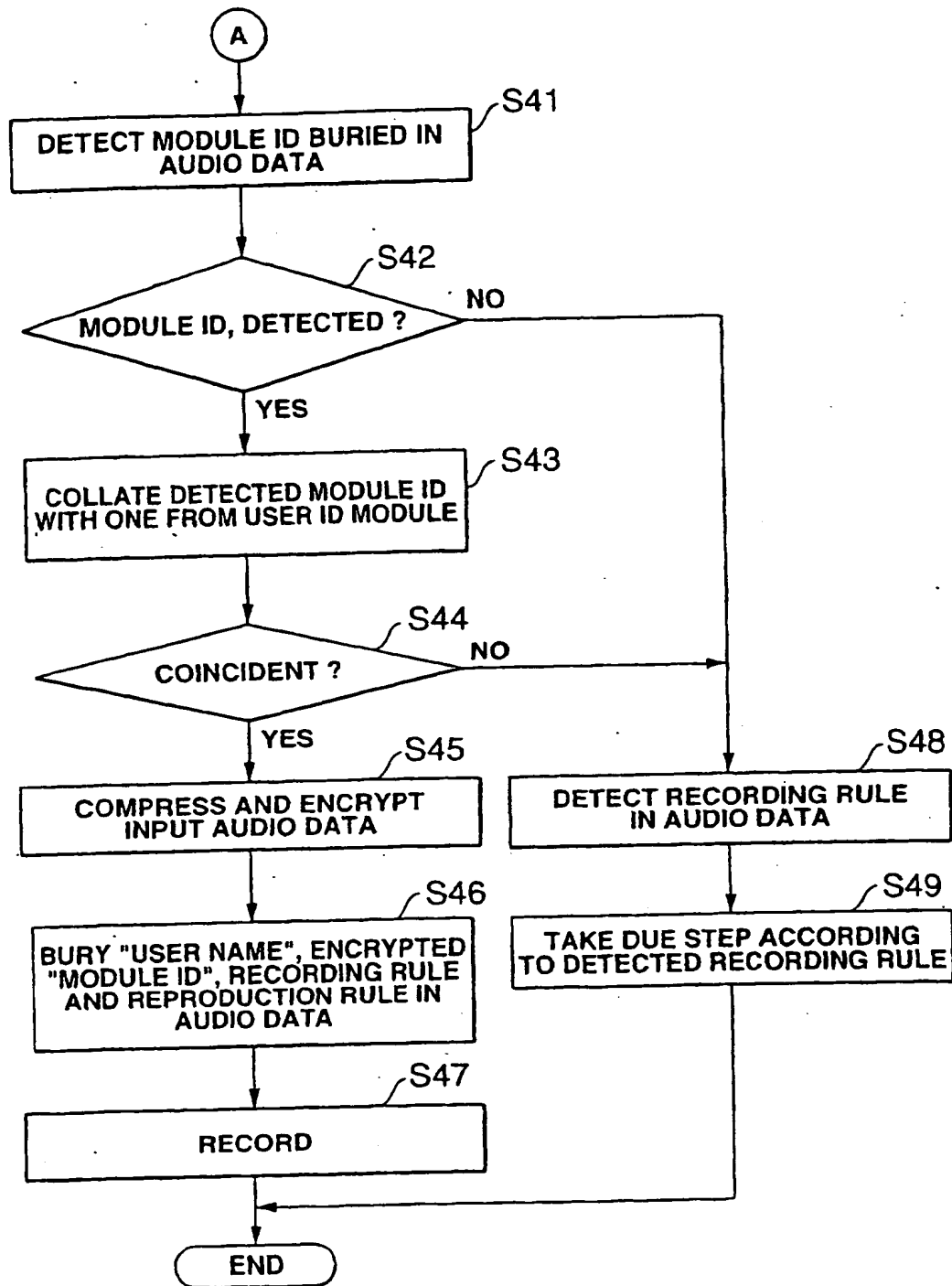


FIG.7

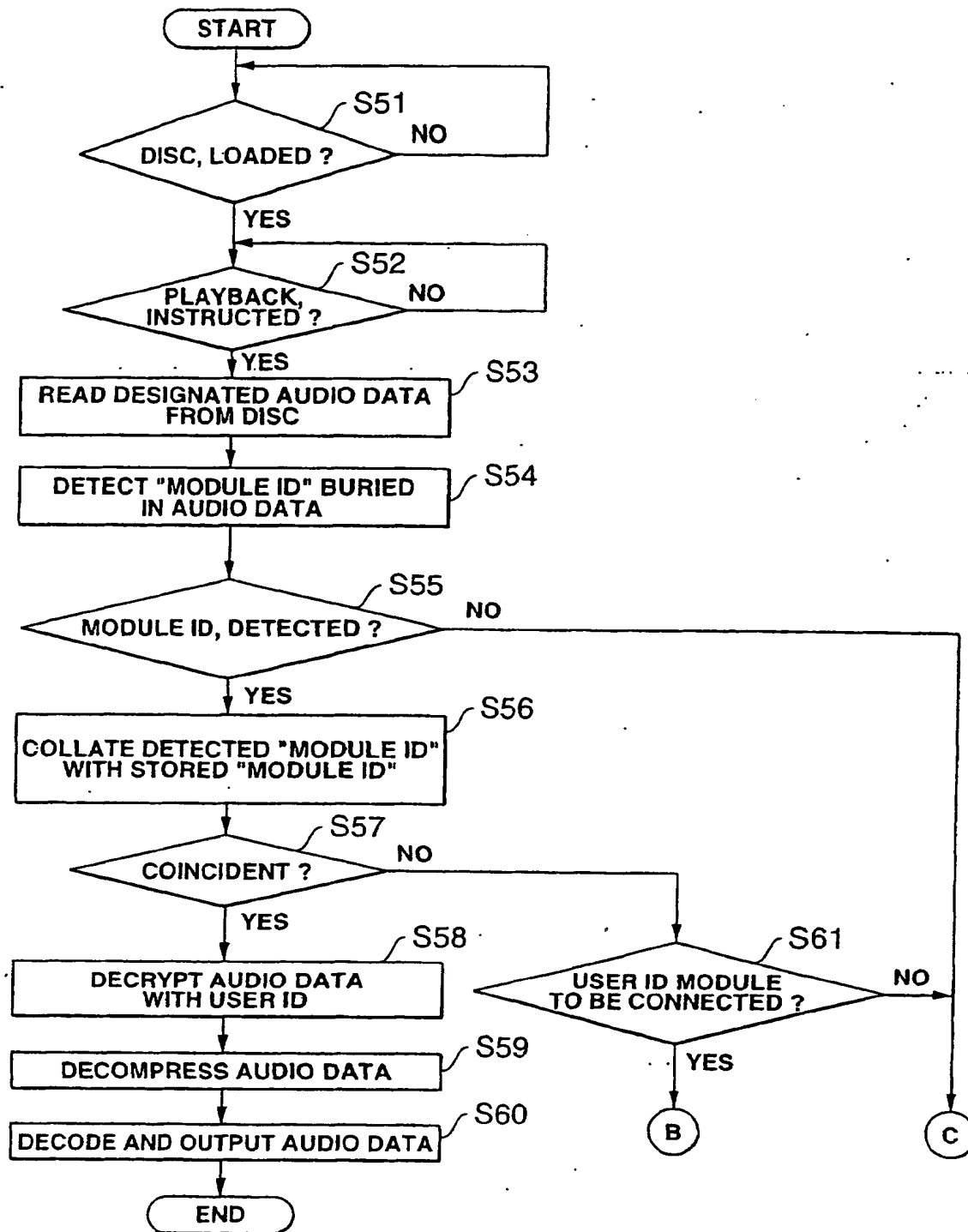


FIG.8

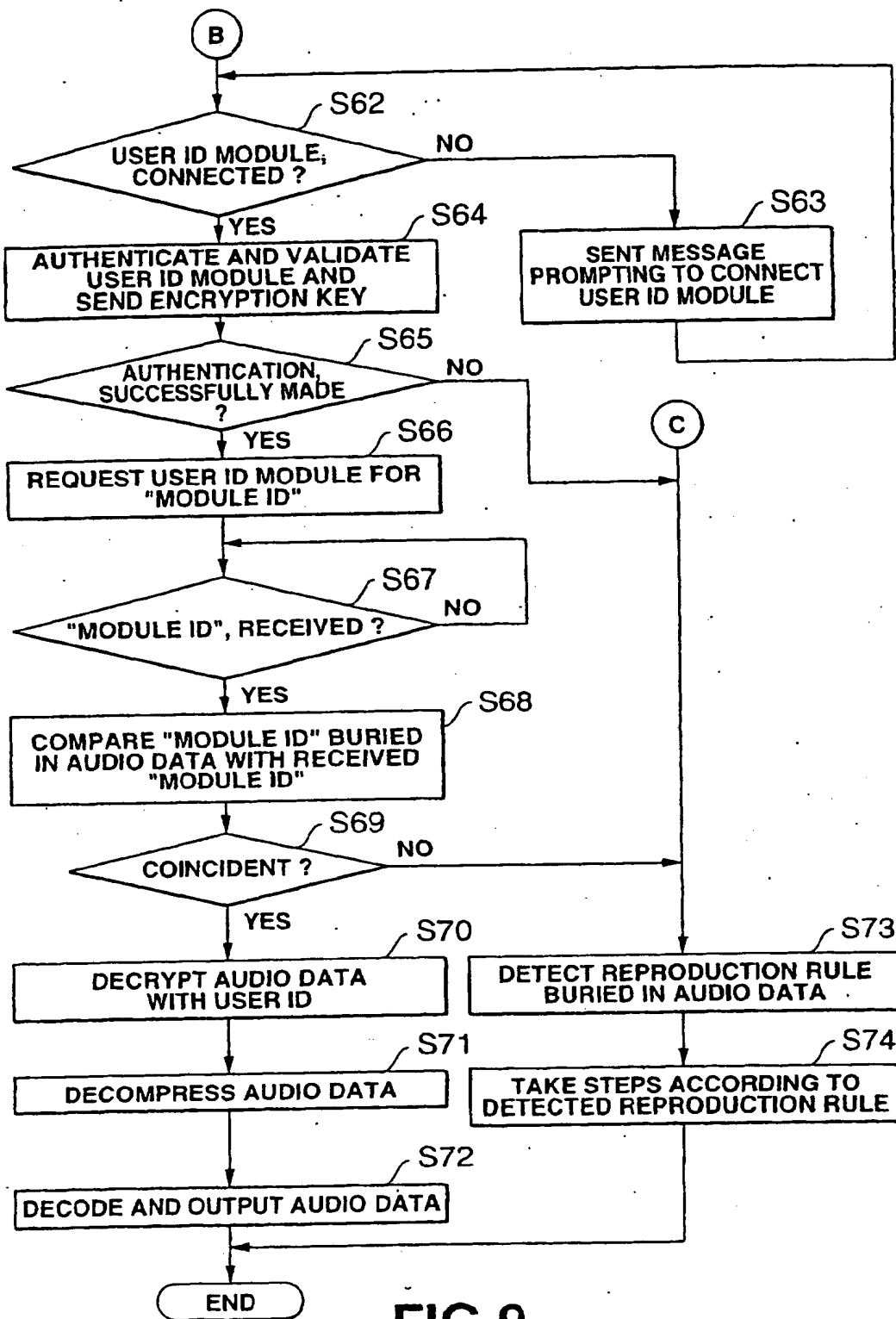


FIG.9

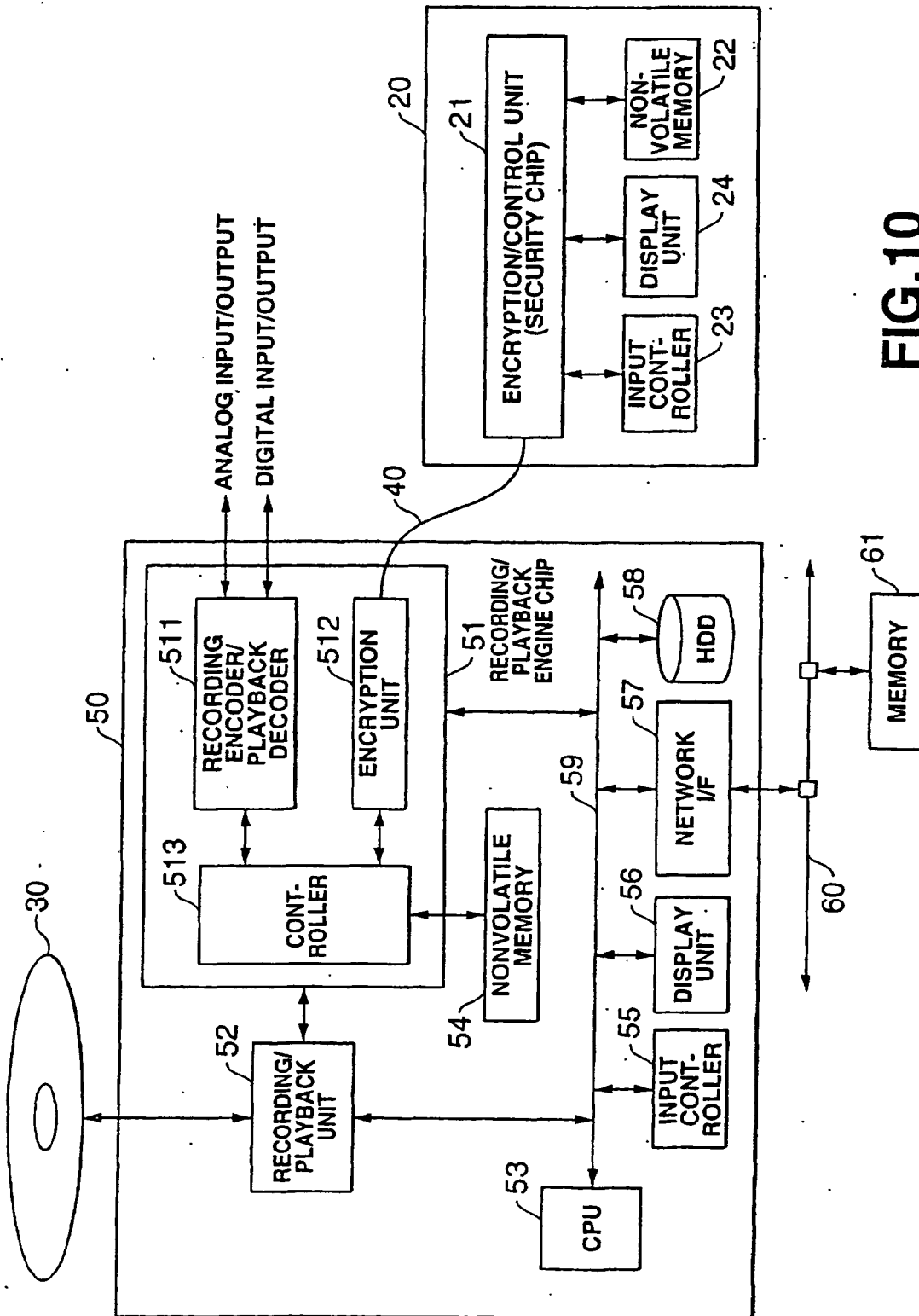


FIG.10

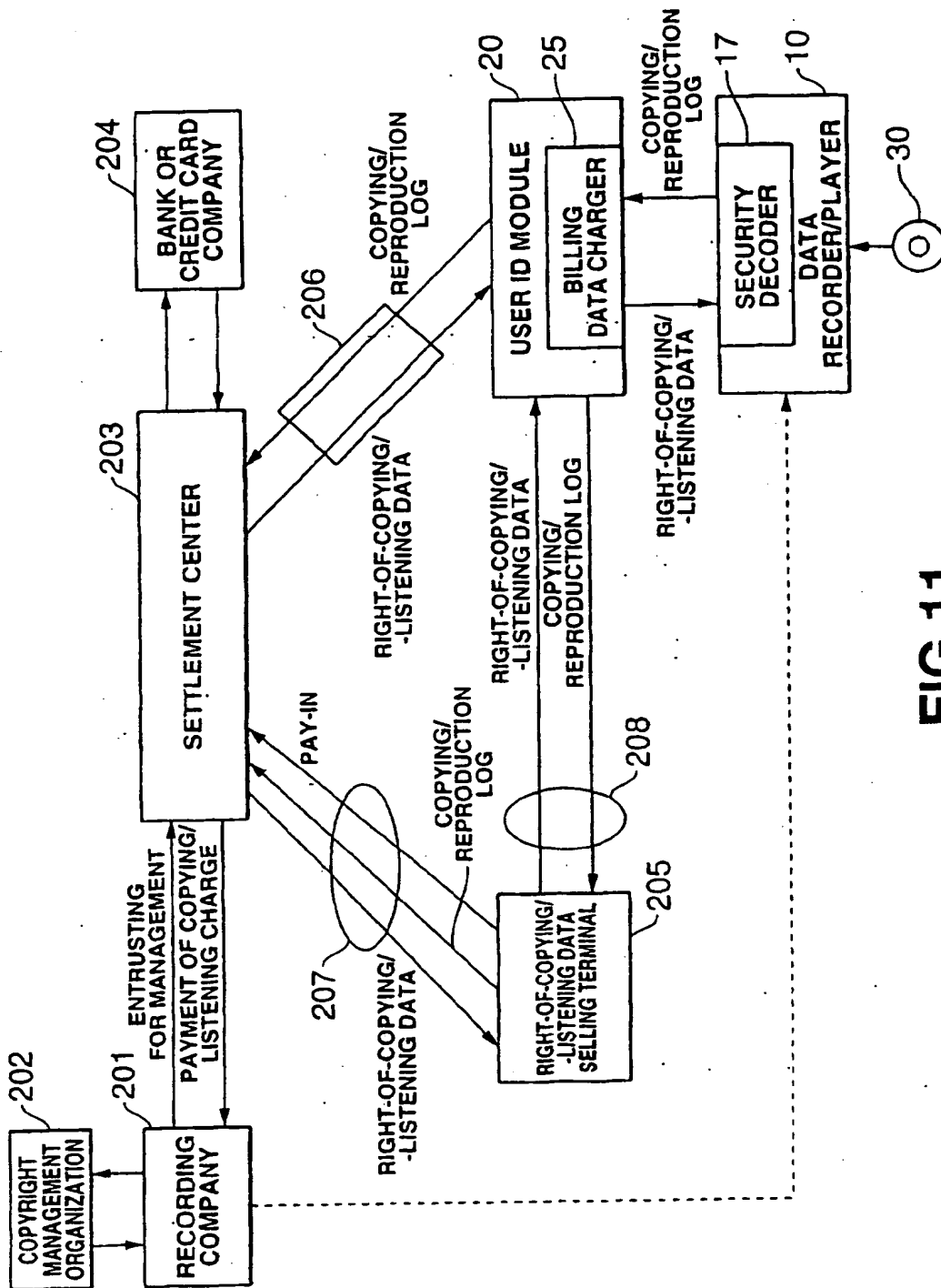


FIG.11

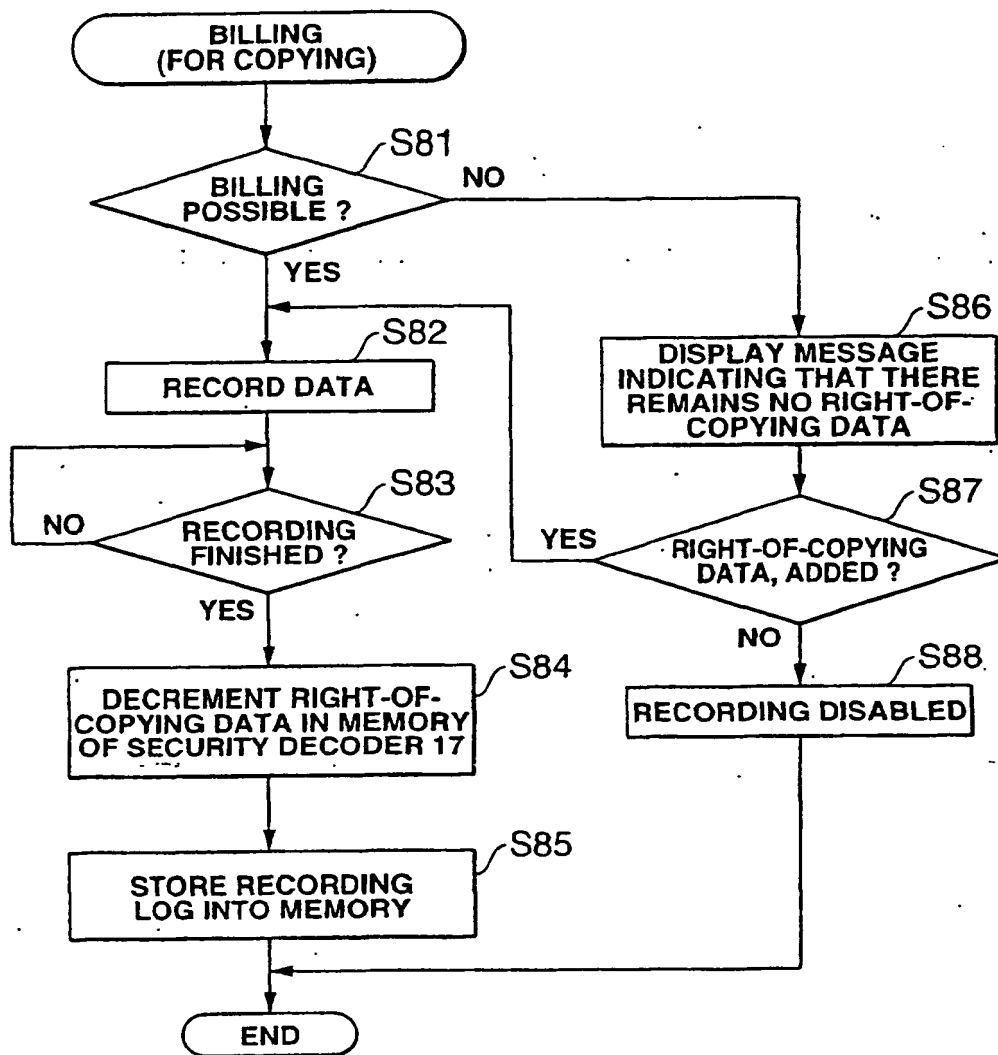


FIG.12

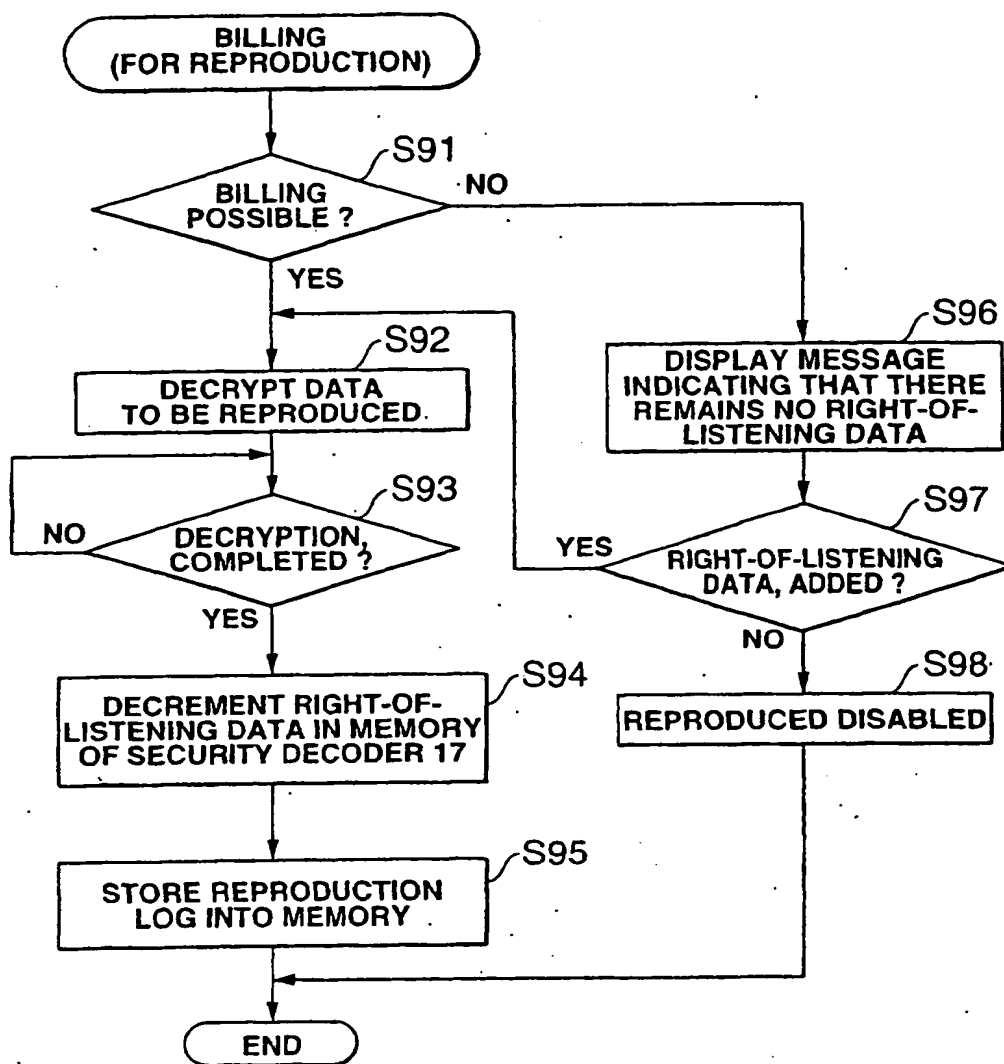


FIG.13

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP01/06183

A. CLASSIFICATION OF SUBJECT MATTER Int.Cl ⁷ G11B 20/10, G10F 3/06, G06F 17/60, G10K 15/02		
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) Int.Cl ⁷ G11B 20/10, H04N 5/91, G10F 3/06, G06F 17/60, G10K 15/02		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2001 Kokai Jitsuyo Shinan Koho 1971-2001 Jitsuyo Shinan Toroku Koho 1996-2001		
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 11-238306 A (Fujitsu Limited), 31 August, 1999 (31.08.99), Full text; Figs. 1 to 18 & EP 000930616 A2 & CN 001227948 A	1-75
Y	JP 10-208388 A (Victor Company of Japan, Limited), 07 August, 1998 (07.08.98), Full text; Figs. 1 to 7 & EP 000853315 A2 & US 006097814 A1	1-75
Y	JP 11-306672 A (Sony Corporation), 05 November, 1999 (05.11.99), Full text; Figs. 1 to 8 (Family: none)	1-75
Y	JP 2000-113587 A (Sony Corporation), 21 April, 2000 (21.04.00), Full text; Figs. 1 to 10 (Family: none)	1-75
A	JP 2000-195161 A (Victor Company of Japan, Limited), 14 July, 2000 (14.07.00), Full text; Figs. 1 to 11 (Family: none)	1-75
<input checked="" type="checkbox"/> Further documents are listed in the continuation of Box C. <input type="checkbox"/> See patent family annex.		
* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "B" earlier document but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family		
Date of the actual completion of the international search 03 October, 2001 (03.10.01)		Date of mailing of the international search report 16 October, 2001 (16.10.01)
Name and mailing address of the ISA/ Japanese Patent Office		Authorized officer
Facsimile No.		Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP01/06183

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 11-213554 A (Toshiba Corporation), 06 August, 1999 (06.08.99), Full text; Figs. 1 to 22 & CN 001220460 A	7-8, 35-36, 50-51, 68-69
A	JP 2000-156036 A (Sony Corporation), 06 June, 2000 (06.06.00), Full text; Figs. 1 to 5 (Family: none)	20-25, 44-49
A	JP 11-313282 A (Sanyo Electric Co., Ltd.), 09 November, 1999 (09.11.99), Full text; Figs. 1 to 16 & EP 000954173 A1	60-62, 70-72

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

THIS PAGE BLANK (USPTO)

(19) 世界知的所有権機関
国際事務局(43) 国際公開日
2002 年 1 月 24 日 (24.01.2002)

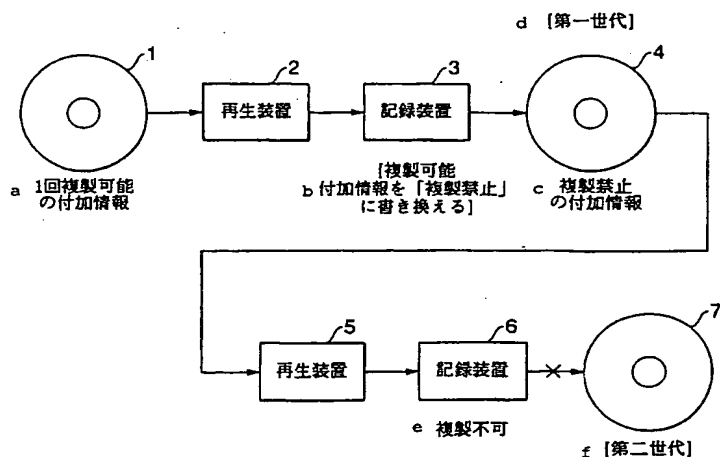
PCT

(10) 国際公開番号
WO 02/07161 A1

- (51) 国際特許分類⁷: G11B 20/10, (INOKUCHI, Tatsuya) [JP/JP]. 佐古 曜一郎 (SAKO, Yoichiro) [JP/JP]. 鳥山 充 (TORIYAMA, Mitsuru) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo (JP).
- (21) 国際出願番号: PCT/JP01/06183
- (22) 国際出願日: 2001 年 7 月 17 日 (17.07.2001)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ: 特願2000-216388 2000 年 7 月 17 日 (17.07.2000) JP (84) 指定国 (広域): ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).
- 特願2000-260467 2000 年 8 月 30 日 (30.08.2000) JP
- (71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 Tokyo (JP).
- 添付公開書類:
— 国際調査報告書
- (72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 猪口達也
- 2 文字コード及び他の略語については、定期発行される各 PCT ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(54) Title: METHOD AND APPARATUS FOR RECORDING AND/OR REPRODUCING DATA AND RECORD MEDIUM

(54) 発明の名称: データ記録及び/又は再生方法及び装置並びに記録媒体



(57) Abstract: A method for recording and/or reproducing data on and/or from a record medium, in which user identification data read out from a record medium where the user identification data along with data is recorded is compared with the user identification data read out from an apparatus in recording or reproducing data on or from the record medium. Recording or reproducing of the recording medium is performed when the user identification data read out from the record medium matches with the user identification data read out from the apparatus.

- a...ADDITIONAL INFORMATION COPIABLE ONCE
b...[REWRITE COPIABLE ADDITIONAL INFORMATION TO "COPY PROHIBITED"]
c...COPY-PROHIBITED ADDITIONAL INFORMATION
d...[FIRST GENERATION]
e...NONCOPIABLE
f...[SECOND GENERATION]
2...REPRODUCER
3...RECORDER
5...REPRODUCER
6...RECORDER



(57) 要約:

本発明は、記録媒体の記録及び／又は再生方法であり、データとともに使用者を特定するための使用者識別データが記録された記録媒体から読み出された使用者識別データと記録媒体の記録又は再生時に装置から読み出された使用者識別データとを比較し、記録媒体から読み出された使用者識別データと装置から読み出された使用者識別データとが一致したときに、記録媒体に記録又は再生を行う。

明細書

データ記録及び／又は再生方法及び装置並びに記録媒体

技術分野

本発明は、著作権管理が必要なコンテンツデータ、例えば、オーディオ情報、画像情報、ゲームプログラム及びデータ、コンピュータプログラムなどのデータを記録し、再生する方法及び記録及び／又は再生装置に関する。

背景技術

デジタルコンテンツの普及に伴い、このデジタルコンテンツについての不正な複製（コピー）による著作権侵害が問題となっている。すなわち、テープ媒体などへのアナログ記録の場合には、オーディオデータや画像データがアナログ的に記録されるため、複製を行うとデータの品質が劣化する。これに対し、デジタル的にオーディオデータや画像データを記録し再生する機器においては、原理的に複製によって情報品質が劣化することがなく、データの複製を多数回繰り返すことさえも品質の劣化無しに可能である。

そのため、デジタル的に処理を行う機器による不正コピーによる損害は、アナログの場合よりさらに大きなものとなり、デジタル的に処理を行う機器における不正コピー防止は、非常に重要になっている。

この問題に対処するため、デジタルコンテンツに複製制御のための情報を付加し、この付加情報を用いて、不正な複製を防止することが行われている。

例えば、この複製の防止のための制御として、オーディオコンテンツについては、1回は複製を認めるが、1回複製されたものからの複製を禁止するSCMS（Serial Copy Management System）と呼ばれる世代制限の複製制御方式による著作権保護施策が、CD（コンパクトディスク）、MD（ミニディスク（登録商標））、DAT（デジタルオーディオテープ）などの装置において用いられてい

る。

このSCMS方式の複製制御方式について、図13を参照して説明する。

例えば、ディスク1には、オリジナルソースのオーディオ信号がデジタル記録されている。デジタルオーディオ信号は、ディスク1に、所定の記録フォーマットで記録されており、SCMS方式による1回複製可能を示す付加情報が、例えばデジタル信号中の特定のエリアに記録されている。

再生装置2は、ディスク1から読み出した信号からデジタルオーディオ信号を再生し、前記の付加情報と共に、記録装置3に伝送する。再生装置2では、通常再生速度（1倍速）に等しい時間分をかけて、デジタルオーディオ信号を記録装置3に伝送する。

このデジタルオーディオ信号を受け取った記録装置3は、デジタルオーディオ信号の付加情報が1回複製可能であるときには、入力デジタル信号の複製が可能であると認識する。記録装置3は、付加情報が1回複製可能であることを確認すると、記録可能なディスク4にデジタル信号を複製記録する。その際に、記録装置3は、付加情報を「1回複製可能」の状態から、「複製禁止」の状態に書き換える。したがって、ディスク4には、デジタル信号が複製記録が行われると共に、その付加情報として、「複製禁止」の情報が記録される。

この1回目の複製記録が行われたディスク4（第1世代のディスク）が再生装置5で再生されて、記録装置6に供給された場合、記録装置6では、付加情報が「複製禁止」となっていることを検知するので、記録可能なディスク7への記録はできなくなる。

このときの複製速度は、再生装置2からのオーディオ信号の伝送速度と等しくなり、オーディオ信号を標準再生時間で再生するとき、すなわち、ノーマル再生速度に等しい速度となる。

ここで、標準再生時間とは、オーディオ信号の場合、実時間再生速度であり、人間が通常知覚するときの再生速度である。例えば、データの場合、標準再生速度は各再生機器により決定され、人間の知覚に関わるものではない。

以上のようにして、SCMS方式では、記録装置で第1世代の複製は許可するが、第1世代の媒体からの第2世代の複製はできないように制御して、著作権保

護を行っている。

SCMS方式の本来の趣旨は、第2世代の複製を禁止することにより、業としての大量の複製が行われてしまうのを防止することにある。現在、一般化している「個人使用の範囲内での複製は自由」という著作権についての概念を否定するものではない。

ところで、最近では、MD（ミニディスク（登録商標））プレーヤや、半導体メモリを内蔵しているカード型メモリプレーヤなどのように、記録再生メディアとして種々のものが登場しており、ユーザも、その日の気分によって、再生メディアとして、MDを用いたり、カード型メモリを用いたりするようになっている。このような現状では複製が頻繁に行われるようになるが、常にオリジナルのメディアからしか複製をすることができないSCMS方式では、個人使用の範囲内での複製であるにもかかわらず、不便を来してしまう。

最近のパーソナルコンピュータは、CDプレーヤの機能を備え、ハードディスクにCDの音楽情報を格納（複製）して再生できるようになっている。カード型メモリへの複製は、複製速度が速いことから、パーソナルコンピュータのハードディスクからの複製が便利であるが、厳密には、ハードディスクからカード型メモリへの複製は、世代としては第2世代になり、ハードディスクに取り込まれた音楽情報のカード型メモリへの複製はできないことになる。

発明の開示

本発明は、以上の点にかんがみ、SCMS方式を採用することなく、個人使用の範囲での複製は自由にし、かつ、業とした不正な複製を有効に防止することができる方法及び装置を提供することを目的とする。

本発明は、記録媒体の記録及び／又は再生方法であり、データとともに使用者を特定するための使用者識別データが記録された記録媒体から読み出された使用者識別データと記録媒体の記録又は再生時に装置から読み出された使用者識別データとを比較し、記録媒体から読み出された使用者識別データと装置から読み出された使用者識別データとが一致したときに、記録媒体に記録又は再生を行う。

本発明に係る記録媒体の記録装置は、データとともに使用者を特定するための使用者識別データが記録された記録媒体を走査するヘッド部と、使用者識別データが記憶されたメモリと、ヘッド部によって記録媒体から読み出された使用者識別データと上記メモリから読み出された使用者識別データとを比較し、その比較結果に基づいて記録媒体の記録動作を制御する制御部とを備えている。

また、本発明に係る記録媒体の再生装置は、暗号化処理が施されたデータとともに少なくとも使用者を特定するための使用者識別データと再生管理データが記録された記録媒体を走査するヘッド部と、使用者識別データが記憶されたメモリと、ヘッド部によって記録媒体から読み出された使用者識別データとメモリから読み出された使用者識別データとを比較し、その比較結果に基づいて記録媒体の再生動作を制御する制御部とを備えている。

さらに、本発明は、データの複製制御方法であり、使用者を特定するための使用者識別データが少なくとも埋めこまれたデータから読み出された上記使用者識別データと上記データの複製動作を行う際に装置から読み出された使用者識別データとを比較し、データから抽出された使用者識別データと装置から読み出された使用者識別データとが一致したときに、データの出力制御を行う。

本発明に係るデータの再生方法は、少なくとも使用者を特定するための使用者識別データが埋めこまれたデータから抽出された使用者識別データとデータの再生時に装置から読み出された使用者識別データを比較し、データから抽出された使用者識別データと装置から読み出された使用者識別データとが一致したときに、データの再生を行う。

本発明の更に他の目的、本発明によって得られる具体的な利点は、以下に説明される実施例の説明から一層明らかにされるであろう。

図面の簡単な説明

図 1 は、SCMS 方式による複製世代制限方法を説明するための図である。

図 2 は、本発明の第 1 の実施の形態を示すブロック図である。

図 3 は、本発明の第 1 の実施の形態の動作説明のためのフローチャートである。

図 4 は、本発明の第 1 の実施の形態の動作説明のためのフローチャートである。

図 5 は、本発明の第 1 の実施の形態の動作説明のためのフローチャートである。

図 6 は、本発明の第 1 の実施の形態における記録処理の説明のためのフローチャートの一部である。

図 7 は、本発明の第 1 の実施の形態における記録処理の説明のためのフローチャートの一部である。

図 8 は、本発明の第 1 の実施の形態における再生処理の説明のためのフローチャートの一部である。

図 9 は、本発明の第 1 の実施の形態における再生処理の説明のためのフローチャートの一部である。

図 10 は、本発明の第 2 の実施の形態のブロック図である。

図 11 は、本発明の実施の形態における課金処理システムの全体の概要を説明するための図である。

図 12 は、本発明の実施の形態における記録時（複製時）の課金処理を説明するためのフローチャートである。

図 13 は、本発明の実施の形態における再生時の課金処理を説明するためのフローチャートである。

発明を実施するための最良の形態

以下、本発明に係るデータ記録再生方法及び装置の具体的な例をディスク記録媒体にオーディオ信号を記録し、再生する場合を例にとって、図面を参照しながら説明する。

図 2 は、本発明に係るデータ記録再生装置の第 1 の実施の形態を適用した記録再生システムを示すブロック図である。

図 2 に示す記録再生システムは、図 2 に示すように、本発明に係るデータ記録再生装置 10 と、使用者識別情報提供装置 20 とからなる。使用者識別情報提供装置 20 は、以下の説明においては、ユーザ ID モジュールと称する。この実施の形態においては、データ記録再生装置 10 には、ユーザ ID モジュール 20 を

接続するための端子が、必ず設けられている。この接続端子を通じて、データ記録再生装置 10 とユーザ ID モジュール 20 との間でやり取りする情報は、安全のため暗号化される。

データ記録再生装置 10 は、記録再生用信号処理部（以下、記録再生エンジンチップと称する。）11 と、記録／再生装置部 12 と、システム制御部 13 と、不揮発性メモリ 14 と、入力操作部 15 と、表示部 16 とを備えている。記録再生エンジンチップ 11 は、機能的には、記録エンコード／再生デコード処理部 111 と、ユーザ ID モジュール 20 との間で、暗号化を伴う通信バスを確立して通信を行うための暗号処理部 112 と、制御部 113 とを備えている。

記録再生エンジンチップ 11 の記録エンコード／再生デコード処理部 111 は、システム制御部 13 の制御を受けて、記録時には、これに対して入力されるアナログオーディオ信号あるいはデジタルオーディオ信号を、後述のように記録エンコード処理して、記録／再生装置部 12 に出力し、再生時には、記録／再生装置部 12 からの再生データを後述のように再生デコードして、アナログオーディオ信号あるいはデジタルオーディオ信号として出力する。

記録再生エンジンチップ 11 の暗号化処理部 112 は、ユーザ ID モジュール 20 に対して、図 2 に示す例では、ケーブル 40 を通じて接続される。この場合、暗号化処理部 112 は、システム制御部 13 の制御の下、ユーザ ID モジュール 20 との間で認証作業を行う認証機能を備え、認証がとれたときに、ユーザ ID モジュール 20 との間に通信路を確立する。この場合に、正規の装置 10 であるように見せかける「なりすまし」等の不正行為を防止するため、装置 10 とモジュール 20 との間で通信を行う前に、装置 10 とモジュール 20 との間で暗号化及び暗号解除のための新しい暗号鍵の伝達を行い、この新しい暗号鍵を用いて装置 10 とモジュール 20 との間で通信されるデータを暗号化する。

記録再生エンジンチップ 11 の制御部 113 は、システム制御部 13 からの制御信号に応じて記録エンコード／再生デコード処理部 111 と、暗号処理部 112 を動作制御すると共に、この制御部 113 に対して接続される不揮発性メモリ 14 に対する使用者識別情報の、書き込み、読み出しを制御する。

記録／再生装置部 12 は、システム制御部 13 による制御を受けて、記録再生

エンジンチップ 11 からの記録信号を、ディスク 30 に記録し、また、ディスク 30 から読み出したデータを、記録再生エンジンチップ 11 に供給する。

システム制御部 13 は、入力操作部 15 を通じた使用者の入力指示に従った制御を行い、また、必要な表示用データを表示部 16 に送って、表示部 16 の画面に表示する。表示部 16 の表示素子としては、液晶ディスプレイなどが用いられる。

ユーザ ID モジュール 20 は、一つのデータ記録再生装置 10 に、一つ付属するもので、使用者識別情報（以下、ユーザ ID という）をデータ記録再生装置 10 に供給するものである。ユーザ ID モジュール 20 は、暗号処理及び制御部（以下、セキュアチップと称する）21 と、不揮発性メモリ 22 と、入力操作部 23 と、表示部 24 とを備えている。

セキュアチップ 21 は、記録再生エンジンチップ 11 との間で認証作業を行う機能を備え、認証がとれたときに、記録再生エンジンチップ 11 との間に通信路を確立する。この際に、上述した「なりすまし」等の不正行為を防止するため、装置 10 とモジュール 20 との間で通信を行う前に、装置 10 とモジュール 20 との間で暗号化及び暗号解除のための新しい暗号鍵の伝達を行う。

不揮発性メモリ 22 には、予め工場出荷時に、各ユーザ ID モジュール 20 に、固有のモジュール識別情報（以下、モジュール ID と称する）、例えば固有の数値が書き込まれている。

使用者は、データ記録再生装置 10 を購入したときに、それに付属しているユーザ ID モジュール 20 に、入力操作部 23 を通じて、表示部 24 の画面で確認しながら、「ユーザ名」を入力して登録する。

[ユーザ ID モジュール 20 へのユーザ名の登録]

図 3 は、このユーザ ID モジュール 20 への「ユーザ名」の登録のための処理手順を示すフローチャートである。

まず、ユーザ ID モジュール 20 は、「ユーザ名」の入力するための画面を、表示部 24 に表示し、使用者に、ユーザ ID モジュール 20 への「ユーザ名」の入力を促す（ステップ S1）。表示部 24 の表示に基づいて、使用者が、入力操作部 23 を用いてユーザ名を入力すると、ユーザ ID モジュール 20 は、入力操

作部 23 によるユーザ名の入力完了を確認した後（ステップ S 2）、入力された「ユーザ名」を、不揮発性メモリ 22 に格納する。以上の処理は、セキュアチップ 21 が実行するものである。

なお、以上のようにして入力されて登録されたユーザ名は、入力操作部 23 を通じた登録ユーザ名の確認操作が行われたときに、不揮発性メモリ 22 から読み出されて、表示部 24 の画面に表示されて、確認することができるようにされている。

こうして、入力された「ユーザ名」と、不揮発性メモリ 22 に予め記憶されていた「モジュール ID」とが、1 対 1 に対応付けられることにより、実質的にモジュール ID がユーザ ID としての意味を有することになる。つまり、ユーザ ID は、本発明においては、モジュール ID とユーザ名との両方を含む概念を意味する場合と、モジュール ID のみからなる概念を意味する場合の 2 通りの場合がある。

〔データ記録再生装置へのユーザ ID の登録〕

以上のようにして、ユーザ名がユーザ ID モジュール 20 に登録された後には、使用者は、ユーザ ID モジュール 20 をデータ記録再生装置 10 に接続して、データ記録再生装置 10 に対するユーザ ID 登録を行う必要がある。

図 4 及び図 5 は、ユーザ ID モジュール 20 を用いて、データ記録再生装置 10 にユーザ ID の登録をする処理手順を示すフローチャートである。図 4 は、このときの、ユーザ ID モジュール 20 側での処理であり、また、図 5 は、データ記録再生装置 10 側での処理である。

＜ユーザ ID モジュール 20 側の処理動作＞

ユーザ ID モジュール 20 では、図 4 に示すように、先ず、データ記録再生装置 10 に接続されたかどうか判別する（ステップ S 11）。ステップ S 11 で接続されていないと判別されたときには、データ記録再生装置 10 が接続されていないことを使用者に表示された一覧表 4 に表示するなどして告知して、使用者に装置 10 の接続を促すようにする（ステップ S 12）。

データ記録再生装置 10 にユーザ ID モジュール 20 が接続されていることが検知されたときには、使用者による入力操作部 23 を通じた「登録指示」を待ち

(ステップS 1 3)、登録指示が受け付けられたことを検知したときには、データ記録再生装置10の記録再生エンジンチップ11との間での認証確認すると共に、暗号鍵の伝達を行う(ステップS 1 4)。

記録再生エンジンチップ11との間で認証確認がとれて、通信路が確立できたか否か判別し(ステップS 1 5)、認証ができずに、通信路が確立できなかったときには、表示部24にエラー表示をして(ステップS 1 7)、この処理ルーチンを終了する。ステップS 1 5で通信路が確立できたときには、不揮発性メモリ22からモジュールID及びユーザ名を読み出し、暗号化して、データ記録再生装置10に対して、登録命令と共に送信する(ステップS 1 6)。

<データ記録再生装置10側の処理動作>

一方、データ記録再生装置10側においては、図5に示すように、先ず、ユーザIDモジュール20が接続されるのを待ち、モジュール20が接続されたことを判別すると(ステップS 2 1)、記録再生エンジンチップ11は、ユーザIDモジュール20の間での認証確認すると共に、暗号鍵の伝達を行う(ステップS 2 2)。

認証確認がとれて、通信路が確立できたか否か判別し(ステップS 2 3)、ステップS 2 3で認証ができずに、通信路が確立できなかったときには、表示部16にエラー表示をして(ステップS 2 6)、この処理ルーチンを終了する。

ステップS 2 3で通信路が確立できた判別されたときには、ユーザIDモジュール20からの「モジュールID」及び「ユーザ名」を含む登録命令の受信を待ち(ステップS 2 4)、受信を確認したら、記録再生エンジンチップ11は、不揮発性メモリ14に、受信したモジュールID及びユーザ名を格納して、所有者登録をする(ステップS 2 5)。

なお、以上のようにして入力されて登録されたユーザ名は、入力操作部15を通じた登録ユーザ名の確認操作が行われたときに、不揮発性メモリ14から読み出されて、表示部16の画面に表示されて、確認することができるようになっている。

データ記録再生装置10のユーザIDは、一旦登録されたものであっても、ユーザIDモジュール20を用いて再登録することにより、別のユーザIDに設定

し直すこともできる。

〔データ記録再生装置 10 での録音処理動作〕

次に、データ記録再生装置 10 での録音処理動作を図 6 及び図 7 に示すフローチャートを参照しながら説明する。

この実施の形態においては、録音をする際には、データ記録再生装置 10 には、ユーザ ID モジュール 20 を接続しておく必要がある。すなわち、データ記録再生装置 10 は、まず、ユーザ ID モジュール 20 が接続されているかどうか判別する（ステップ S 3 1）。ステップ S 3 1 でユーザ ID モジュール 20 が接続されていないと判別されたときには、ユーザ ID モジュール 20 が接続されていないことを表示部 1 6 に表示するなどして使用者に告知して、モジュール 20 の接続を促すようにする（ステップ S 3 2）。例えば「ユーザ ID モジュールが接続されていないので記録はできません。ユーザ ID モジュールを接続して下さい。」というメッセージを表示部 1 6 に表示したり、音声によるメッセージとして放音することによって使用者に告知する。

ステップ S 3 1 でデータ記録再生装置 10 にユーザ ID モジュール 20 が接続されていることが検知されたときには、使用者による入力操作部 1 5 を通じた

「録音指示」を待ち（ステップ S 3 3）、ステップ S 3 3 で「録音指示」が受け付けられたことを検知したときには、データ記録再生装置 10 のシステム制御部 1 3 は、録音命令を記録再生エンジンチップ 1 1 や記録／再生装置部 1 2 に供給し、録音開始準備状態とする（ステップ S 3 4）。

次に、記録再生エンジンチップ 1 1 は、ユーザ ID モジュール 20 のセキュアチップ 2 1 との間での認証確認すると共に、暗号鍵の伝達を行う（ステップ S 3 5）。認証確認がとれて、通信路が確立できたか否か判別し（ステップ S 3 6）、ステップ S 3 6 で認証ができずに、通信路が確立できなかったときには、録音動作を中止し（ステップ S 3 7）、その後、表示部 2 4 にエラー表示をして（ステップ S 3 8）、この処理ルーチンを終了する。

ステップ S 3 6 で、通信路が確立できたと判別したときには、記録再生エンジンチップ 1 1 は、ユーザ ID モジュール 20 に対して、ユーザ ID、つまり、この例の場合には、モジュール ID 及びユーザ名の送信要求を出す（ステップ S 3

9)。

ユーザIDモジュール20のセキュアチップ21は、ユーザIDの送信要求に対して、不揮発性メモリ22からモジュールID及びユーザ名を読み出し、暗号化して、データ記録再生装置10に対して送信する。データ記録再生装置10の記録再生エンジンチップ11は、このモジュールID及びユーザ名の受信したか否かをを確認する(ステップS40)。

次に、ステップS31で0で受信を確認した後は、オーディオデータ中に埋め込まれているモジュールIDの検出を行い(ステップS41)、モジュールIDが検出できたか否かを判別する(ステップS42)。ステップS42でモジュールIDが検出できたときには、検出されたモジュールIDと、ユーザIDモジュール20から取得したモジュールIDとを比較照合する(ステップS43)。

ステップS43でのその比較照合の結果、両モジュールIDが一致したか否かを判別し(ステップS44)、両モジュールIDが一致したときには、記録許可となり、入力オーディオデータに圧縮処理を施し、受信したユーザIDを暗号鍵とした暗号化処理する(ステップS45)。

この場合、暗号鍵としては、ユーザ名のみを用いる場合、モジュールIDのみを用いる場合、又はユーザ名及びモジュールIDの両者を用いる場合のいずれであってもよい。

ステップS45で圧縮及び暗号化処理したオーディオデータ中に、ユーザIDモジュール20から取得した「ユーザ名」と、「モジュールID」とを埋め込む(ステップS46)。この場合に、モジュールIDは暗号化して埋め込む。モジュールIDを暗号化して埋め込むのはユーザIDの秘匿性を高めるためである。ステップS46では、さらに、後述する記録ルールや再生ルールを、記録対象のオーディオデータに埋め込む。

以上のようにして、暗号化し、ユーザIDなどを埋め込んだオーディオデータは、記録媒体としてのディスク30に記録する(ステップS47)。

一方、ステップS42でモジュールIDが検出できなかったときと、ステップS44でオーディオデータから検出されたモジュールIDとユーザIDモジュール20からのモジュールIDとが不一致であったときには、オーディオデータ中

に埋め込まれている記録条件（記録ルール）を検出し（ステップS48）、その検出した記録ルールにしたがった処理を行う（ステップS49）。

この記録ルールの情報の埋め込み処理としては、電子透かし処理と呼ばれている処理や、その他の埋め込み処理を用いることができる。また、オーディオデータ中に埋め込むのではなく、TOC（Table Of Contents）データが記録されているエリアなどのオーディオデータが記録されている記録エリアとは別の記録エリアや、サブコードのエリアなどに記録するようにしてもよい。

このとき埋め込む記録ルールとしては、例えば、

R1「無料で記録（複製）可能」

R2「記録（複製）は有料」

R3「記録（複製）はフリー」

R4「記録（複製）は不可」

のうちの一つが選択されて記録されているものである。記録ルールの記録情報としては、記録ルールの内容そのものを記録してもよいが、上述のR1～R4のいずれであるかの情報を記録することもできる。

ここで、R1「無料で記録（複製）可能」は、ユーザIDをオーディオデータに埋め込んで、記録を実行させるものである。これは、この例では、オーサリング装置でレコード会社などにより制作される読み出し専用形式（以下、ROMタイプという）のディスクなどの記録媒体には、所有者無しとしてユーザIDを埋め込まずに記録するので、このROMタイプの記録媒体からのオーディオデータの記録（複製）時の処理となる。

上記R2「記録（複製）は有料」は、課金処理が可能な記録装置において、課金処理が実行できたときに記録を許可するものである。課金処理が不能の記録装置の場合には、記録は不可とされる。なお、課金処理の例については、後述する。

上記R3「記録（複製）はフリー」は、ユーザIDはオーディオデータに記録せずに、記録（複製）を行う処理である。さらに、R4「記録（複製）は不可」は、全く記録（複製）は不可であることを意味している。

上述のように、記録ルールは、ユーザIDが不一致の場合だけでなく、記録対象のオーディオデータからユーザIDが検出できなかったときにも適用されるが、

ユーザIDが不一致の場合と、有効なユーザIDが得られない場合とでは、異なる記録ルールを記録しておくようにしてもよい。

また、後述するように、この実施の形態では、再生時には、オーディオデータ中に埋め込まれたユーザIDと、不揮発性メモリ14に格納されたユーザIDとの照合を行い、両者が一致したときに、そのオーディオデータの再生が可能となる。この実施の形態では、再生時にオーディオデータからユーザIDが検出できなかったとき、また、再生時での照合の結果、ユーザIDが不一致であるときに、どのように処理するか再生ルール（再生条件）も、ステップS46で、オーディオデータ中に埋め込むようにする。

この再生ルールの情報の埋め込み処理としては、記録ルールと同様に、電子透かし処理と呼ばれている処理や、その他の周知の埋め込み処理を用いることができる。また、オーディオデータ中に埋め込むのではなく、TOC (Table Of Contents) データなどのオーディオデータが記録されている記録エリアとは別の記録エリアや、サブコードのエリアなどに記録するようにしてもよい。

この再生時にユーザIDが不一致の場合の再生ルールとしては、例えば、

PB1 「無料再生可能」

PB2 「再生禁止（再生不可）」

PB3 「再生は有料」

PB4 「制限付きで再生可能」

のうちの一つが選択されて記録されるものである。再生ルールの記録情報としては、再生ルールの内容そのものを記録してもよいが、上述のPB1～PB4のいずれであるかの情報を記録することもできる。

ここで、上記PB1「無料再生可能」の場合には、再生装置に登録されたユーザIDに関係なく、常に、オーディオデータの再生可能となり、PB2「再生禁止（再生不可）」の場合には、再生装置に登録されたユーザIDと不一致の場合、常に、オーディオデータの再生が禁止される。前述したように、この例では、オーディオ再生装置でレコード会社などにより制作されるROMタイプのディスクなどの記録媒体には、ユーザIDを埋め込まずに記録するので、再生オーディオデ

ータから有効なユーザIDが得られない場合として、上記PB①のルールが記録される。

また、上記PB3「再生は有料」の場合には、課金処理が可能な再生装置において、課金処理が実行できたときに、オーディオデータの再生を許可するものである。課金処理が不能の再生装置の場合には、オーディオデータの再生は不可とされる。なお、課金処理の例については、後述する。

上記PB4「制限付きで再生可能」は、例えば、全部又は一部の試聴モードを許可し、その試聴モードの後には、上記PB2又はPB3のルールとするものである。ここで、試聴モードとは、

- a) n回、例えば1回だけ無料再生可能
- b) m秒分だけ無料再生可能
- c) さわり部分やさび部分だけ無料再生可能

を意味する。

このPB4「制限付き再生可能」の再生ルールで、前記a)やb)を採用する場合には、再生装置は、例えば、ISRC (International Standard Recording Code) などのコンテンツID (識別コード) に対応させて、そのコンテンツIDで識別されるオーディオデータの試聴履歴の情報、例えば試聴回数や、試聴秒数などを記録するようにする。

この実施の形態では、後述の再生処理で説明するように、この再生ルールは、再生時にユーザIDが不一致の場合だけでなく、再生オーディオデータから、有効なユーザIDが得られないときにも共通に適用される。しかし、ユーザIDが不一致の場合と、有効なユーザIDが得られない場合とでは、異なる再生ルールを記録するようにしてもよい。

例えば、オーサリング装置でレコード会社などにより制作されるROMタイプのディスクなどの記録媒体にも、ユーザIDとして、例えば「ORIGINAL」などの特定のID、すなわち、記録媒体がオリジナルであることを示す識別データが記録される場合には、再生装置は、その特定のIDを検出したときには、自己の装置のユーザIDと不一致の場合でも、再生許可すべきである。したがって、再生ルールが埋め込まれるものとした場合には、その再生ルールは、「再生

可能」とされる。

一方、このように特定のユーザIDが、ROMタイプのディスクなどの記録媒体の記録データに埋め込まれるなどして、記録データに付随して記録されると定められている場合には、再生装置において、有効なユーザIDが得られないときには、そのオーディオデータは、不正に記録されたものであるとすることができると。したがって、その時の再生ルールは再生不可とするのがよい。

オーサリング装置でレコード会社などにより制作されるROMタイプのディスクなどの記録媒体には、ユーザIDを記録しないと定められている場合には、上述のような再生ルールのうちの一つを共通に用いることができる。

[データ記録再生装置10での再生処理動作]

次に、以上のようにして録音されたオーディオデータを、データ記録再生装置10で再生する場合の処理動作を図8及び図9のフローチャートを参照しながら説明する。

まず、記録済みのディスクが装填されるのを待ち、装填されたことを判別すると(ステップS51)、記録再生エンジンチップ11は、使用者からの再生指示を待つ。そして、使用者からの入力操作部15による再生指示を確認すると(ステップS52)、ディスクから再生指示のあったオーディオデータを読み出す(ステップS53)。

読み出されたオーディオデータに埋め込まれているユーザIDを検出する。ユーザIDのうちの、この例では、暗号化されているモジュールIDの暗号を解除して検出する(ステップS54)。モジュールIDが検出できたか否かを判別し(ステップS55)、検出できなかったときには、再生オーディオデータに埋め込まれている再生ルールを検出し(ステップS73)、その検出された再生ルールに従った処理を行う(ステップS74)。

ステップS55で、モジュールIDを検出することができたと判別されたときには、その検出されたモジュールIDと、不揮発性メモリ14に記憶されているモジュールIDとを比較照合する(ステップS56)。

両モジュールIDが一致しているかどうか判別し(ステップS57)、ステップS57で両モジュールIDが一致しているときには、ユーザIDが用いられて

暗号化されているオーディオデータの暗号を解き（ステップS 5 8）、オーディオデータの圧縮を解凍、即ち、慎重処理する（ステップS 5 9）。伸張されたオーディオデータを復号して、再生出力する（ステップS 6 0）。

一方、ステップS 5 7で、ディスク30から読み出したデータから検出されたモジュールIDと、不揮発性メモリ14から読み出されたモジュールIDとが不一致であると判別されたときには、ユーザに、ユーザIDモジュール20を接続させる設定になっているかどうかを判別し、その判別の結果、ユーザIDモジュールを接続させる設定になっていなければ、再生オーディオデータに埋め込まれている再生ルールを検出し（ステップS 7 3）、その検出された再生ルールに従った処理を行う（ステップS 7 4）。この例では、例えばディスク30の再生が禁止となる。

この場合の再生禁止には、装置10が正常な再生出力が行われないことも含まれる。つまり、装置10からの再生出力としてノイズが出力される場合の他、装置10からの再生出力に代えて、「違法に複製された記録媒体からの再生である」旨のメッセージを、オーディオ出力として装置10から送出するようにしてもよい。

ステップS 6 1で、ユーザに、ユーザIDモジュールを接続させる設定になっていると判別されたときには、データ記録再生装置10は、ユーザIDモジュール20が接続されているかどうか判別する（ステップS 6 2）。ステップS 6 2で接続されていないと判別されたときには、ユーザIDモジュール20が接続されていないことを使用者に報知して、モジュール20の接続を促すようにする（ステップS 6 3）。

データ記録再生装置10にユーザIDモジュール20が接続されていることが検知されたときには、記録再生エンジンチップ11は、ユーザIDモジュール20との間での認証確認すると共に、暗号鍵の伝達を行う（ステップS 6 4）。認証確認がとれて、チップ11とモジュール20との間で通信路が確立できたか否か判別し（ステップS 6 5）、認証ができずに、チップ11とモジュール20との間で通信路が確立できなかったときには、オーディオデータに埋め込まれた再生ルールに従った処理を行う（ステップS 7 3、ステップS 7 4）。この例では、

前述のようにディスク 30 の再生が禁止となる。

ステップ S 6 5 で、チップ 1 1 とモジュール 2 0 との間で通信路が確立できたと判別したときには、記録再生エンジンチップ 1 1 は、ユーザ ID モジュール 2 0 に対して、ユーザ ID のうちの、この例の場合には、モジュール ID の送信要求を出す（ステップ S 6 6）。

ユーザ ID モジュール 2 0 のセキュアチップ 2 1 は、エンジンチップ 1 1 からのこの送信要求に対して、不揮発性メモリ 2 2 からモジュール ID を読み出し、暗号化して、データ記録再生装置 1 0 に対して送信する。データ記録再生装置 1 0 の記録再生エンジンチップ 1 1 は、ユーザ ID モジュール 2 0 から送信されてきたモジュール ID の受信を確認すると（ステップ S 6 7）、ディスク 3 0 から読み出したデータから検出されたモジュール ID と、受信し暗号を解いた又は復号したモジュール ID とを比較照合する（ステップ S 6 8）。

両モジュール ID が一致しているかどうか判別し（ステップ S 6 9）、両モジュール ID が不一致であったときには、オーディオデータに埋め込まれた再生ルールに従った処理を行う（ステップ S 7 3、ステップ S 7 4）。前述したように、この例では、ディスク 3 0 の再生禁止となる。

両モジュール ID が一致したときには、ユーザ ID が用いられて暗号化されているオーディオデータの暗号を解き、即ち復号し（ステップ S 7 0）、オーディオデータの圧縮を解凍、即ち伸張処理する（ステップ S 7 1）。圧縮が解凍された、即ち伸張処理されたオーディオデータを復号して、再生出力する（ステップ S 7 2）。

以上のようにして、この実施の形態においては、記録時に、登録されたユーザ ID を記録データに埋め込んで記録し、再生時には、不揮発性メモリ 1 4 に登録されたユーザ ID と、ディスク 3 0 から読み出されたデータから検出されたユーザ ID とを比較して、両ユーザ ID が一致したときに、ディスクから読み出されたデータの正常な再生出力を行うようにしたことにより、個人的な利用形態に限って複製を可能にすることができる。

上述の実施の形態では、記録時には、ユーザ ID モジュール 2 0 を、データ記録再生装置 1 0 に接続した状態ではないと記録を実行することができないように

したので、この点でも、ユーザの個人使用の範囲内での制限をすることができる。

この実施の形態では、記録側に上記のような制限を加えた代わりに、再生側においては、不揮発性メモリ 14 に登録されたユーザ ID と、ディスク 30 から読み出されたデータから検出されたユーザ ID とを比較して、両ユーザ ID が一致しているかどうかを判別するようにしており、記録時のように、ユーザ ID モジュール 20 を接続する必要はなく、再生時におけるユーザの使い勝手が良くなるという効果がある。

例えば、「個人使用の範囲でコピーは自由」ということを具現化する方法として、個人で取得済みの聴取権情報（例えば、その個人が持っているコンテンツの全ての情報）を自分専用の IC カードに記録しておき、コンテンツを再生する際には、必ずその IC カードを再生装置に差し込むようにする方法が考えられる。この場合、IC カードを他人が使えない状態に保つために、一人一枚の IC カードを持つように管理される。

このようにすれば、IC カードが、その個人の全ての聴取権情報を持つので、コンテンツの複製は、全く自由にしても問題がなくなるが、その代わりに、使用者は、再生装置に差し込む IC カードを持ち歩かなければならなくなるという問題がある。

上述の実施の形態の場合には、再生装置には、その IC カードのようなものは不要となるので、非常に便利である。

上述の実施の形態では、記録データは、ユーザ ID を暗号鍵とした暗号を施して記録するようにしているので、再生時には、ユーザ ID が一致したときにしか、記録データの暗号化が解除、復号できなくなり、より個人使用の範囲内での制限を確実にすることができる。

なお、ユーザ ID を暗号鍵そのものとせず、記録データの暗号化の鍵を取得するための情報などのように、暗号化に関連する情報として用いても、同様の効果が得られると期待できる。但し、記録ルール又は再生ルールでユーザ ID が不一致の場合にも記録又は再生を許可している場合には、必ずしもユーザ ID を暗号鍵に用いなくともよい。

上述の実施の形態では、ユーザ ID モジュール 20 からのユーザ ID の情報は、

暗号化してデータ記録再生装置 10 に送るようにしており、このため、ユーザ ID の秘匿性を高めることができるという効果もある。

上述の説明では、記録ルール及び再生ルールをオーディオデータに埋め込んだので、記録ルール及び再生ルールの情報は、オーディオデータから検出するようにするが、記録ルール及び再生ルールの情報が、TOC エリア又 TOC データ内などに記録されていた場合には、記録対象のオーディオデータの記録又は再生動作に先立ち、記録ルール及び再生ルールの情報を取得するようにすればよい。

オーディオデータが圧縮されてブロック化されている場合には、ブロックとブロックの間の隙間に記録ルール及び再生ルールの情報を埋め込むようにすることもできる。その場合には、圧縮デコードのときに、記録ルール及び再生ルールの情報を抽出することができる。

データ記録再生装置 10 が、データの再生と記録が同時にでき、データの複製記録ができるように、記録媒体を同時に複数枚装填できるようにされている場合には、再生側のディスクから記録ルールや再生ルールの情報を予め TOC データや再生データから得るようにすることもできる。

なお、以上の実施の形態では、記録ルール及び再生ルールをオーディオデータ中に必ず記録するように説明したが、予め、システムとして、ユーザ ID が得られなかったとき、また、ユーザ ID が不一致のときの、記録ルール及び再生ルールを、例えば上述のルールのうちの一つに定めておくようにすれば、記録ルール及び再生ルールをオーディオデータ中に記録する必要はなくなる。

[第 2 の実施の形態]

この第 2 の実施の形態は、データ記録再生装置が、パーソナルコンピュータに搭載される場合の例である。図 10 は、この第 2 の実施の形態の場合のシステムのブロック図である。

この第 2 の実施の形態のシステムは、パーソナルコンピュータ 50 と、前述の第 1 の実施の形態の場合に用いたユーザ ID モジュール 20 とにより構成される。

この実施の形態のパーソナルコンピュータ 50 は、ユーザ ID モジュール 20 を接続するための端子を備えている。このモジュール 20 を接続するための端子を通じて、パーソナルコンピュータ 50 とユーザ ID モジュール 20 との間でや

り取りする情報は、全て暗号化されるものである。

パーソナルコンピュータ 50 は、第 1 の実施の形態のデータ記録再生装置 10 と同様に、記録再生エンジン 51 と、記録／再生装置部 52 と、不揮発性メモリ 54 とを備えると共に、システムバス 59 を介して、CPU 53 と、入力操作部 55 と、表示部 56 と、ネットワークインターフェース 57 と、ハードディスク装置 58 とが接続される。システムバス 59 には、記録再生エンジン 51 と、記録及び／又は再生装置部 52 も接続されている。

ネットワークインターフェース 57 は、ネットワーク 60 に接続された記憶装置 61 に対して接続される。ここで、ネットワーク 60 は、ローカルエリアネットワーク（LAN）であっても良いし、インターネットであってもよい。インターネットの場合には、記憶装置 61 は、所定のサーバなどに設けられた記録装置とされる。

この第 2 の実施の形態においても、前述の第 1 の実施の形態と全く同様にして、ユーザ ID モジュール 20 には、ユーザ名が入力登録され、その後、パーソナルコンピュータ 50 にユーザ ID の登録処理が、ユーザ ID モジュール 20 から、パーソナルコンピュータ 50 に対して行われて、不揮発性メモリ 54 には、ユーザ ID が登録されて記憶される。

この第 2 の実施の形態の場合には、記録メディアとしては、第 1 の実施の形態の場合のディスク 30 のみではなく、ハードディスク装置 58 やネットワーク 60 に接続された記憶装置 16 も用いられる。

すなわち、この第 2 の実施の形態の場合の記録における入力ソースと、記録媒体（記録メディア）との組み合わせを示すと、

1. アナログ入力あるいはデジタル入力→ディスク 30
2. アナログ入力あるいはデジタル入力→ハードディスク装置 58
3. アナログ入力あるいはデジタル入力→記憶装置 61
4. ディスク 30→ハードディスク装置 58
5. ディスク 30→記憶装置 61
6. ハードディスク装置 58→ディスク 30
7. ハードディスク装置 58→記憶装置 61

8. 記憶装置 61 → ディスク 30

9. 記憶装置 61 → ハードディスク装置 58

などがある。

これら 9 通りの他にも、ネットワーク 60 上の一つの記憶装置から、他の記憶装置に転送して書き込む処理も、記録処理の一つと考えられる。以上のいずれの記録時においても、この第 2 の実施の形態では、前述の第 1 の実施の形態と同様に、ユーザ ID モジュール 20 が接続されることを条件とすると共に、そのユーザ ID モジュール 20 から取得したユーザ名及びモジュール ID とを、記録データに埋め込んで記録するようにする。この場合に、第 1 の実施の形態と同様に、モジュール ID は、暗号化して記録する。

この場合、ハードディスク装置 58 への記録の場合には、記録再生エンジンチップ 11 で記録エンコードされたデータは、記録／再生装置部 52 を経ることなく、システムバス 59 を通じてハードディスク装置 58 に送られて、ハードディスクに格納される。

記憶装置 61 への記録の場合には、記録再生エンジンチップ 11 で記録エンコードされたデータは、記録／再生装置部 52 を経ることなく、システムバス 59 及びネットワークインターフェース 57 を通じて記憶装置 61 に対してネットワーク 60 に送出され、記憶装置 61 に格納されるようにされる。

ディスク 30、ハードディスク装置 58、記憶装置 62 のいずれからのオーディオデータの再生時においても、前述の第 1 の実施の形態と全く同様に、再生データ中から検出したユーザ ID と、不揮発性メモリ 54 に記憶されていたユーザ ID との照合が行われて、両者が一致したときに、オーディオデータの再生出力を可能とするようにする。

この第 2 の実施の形態の場合にも、上述した第 1 の実施の形態と同様の効果が得られると共に、ハードディスク装置 58 を用いた高速複製が、ユーザの個人使用の範囲内という制限を保持して可能となる。ネットワークを通じた記憶装置へのデータ転送も、一つの記録（複製）態様とすることができるが、それも、ユーザの個人使用の範囲内という制限を保持して可能となる。

[課金処理の例について]

次に、記録ルール及び再生ルールが課金を条件にしている場合に対応する実施の形態を説明する。図 1 1 は、この例の課金処理システムの一例を示すものであり、音楽コンテンツの配付、音楽コンテンツのデータの授受については、省略されている。この実施の形態のデータ記録再生装置 1 0 は、複製記録ができるように構成されている。つまり、あるディスクからのデータを、別のディスクに記録することが可能とされている。

この実施の形態の場合、課金処理のために、記録に際しては複製権データが、再生に際しては聴取権データが、それぞれ使用される。これら複製権データおよび聴取権データは、ICカードや、データ記録再生装置 1 0 に設けられるセキュアデコーダ 1 7 のメモリに格納される。

複製権データ及び聴取権データは、例えば複製可能な度数及び再生可能な度数であり、データ記録再生装置 1 0 が課金対象のコンテンツを記録／再生する度に、それぞれの度数が減算される。

これら複製権データ及び聴取権データは、複製／聴取権データ管理会社の管理下で、ユーザが所有する複製／聴取権データチャージャ又は販売店に設置された複製／聴取権データ販売端末 2 0 5 によって書き替えることが可能とされている。この例では、複製／聴取権データチャージャは、ユーザ ID モジュール 2 0 内に課金データチャージャ 2 5 として設けられている。

課金データチャージャ 2 5 は、データ記録再生装置 1 0 のセキュアデコーダ 1 7 と決済センター 2 0 3 又はレコード店、コンビニエンスストア等に設置されているデータ販売端末 2 0 5 との間に存在して聴取権データ中継器として機能する。

レコード会社 2 0 1、著作権管理機構 2 0 2、ユーザデバイスとしてのデータ記録再生装置 1 0 と関係して、代金決済のために、決済センター 2 0 3 が存在している。決済センター 2 0 3 は、認証／課金サーバを備えている。決済センター 2 0 3 は、銀行、クレジットカード会社 2 0 4 との間で代金の決済を行う。

図 1 1 において、破線で示すように、レコード会社 2 0 1 から配布される、記録再生装置 1 0 が再生する媒体（光ディスク、メモリカード等）には、音楽コンテンツが記録されている。音楽コンテンツの配信の方法は、この他、種々のものが使用できる。また、記録再生装置 1 0 は音楽コンテンツを媒体（光ディスク、

メモリカード等) 30に記録する。

データ記録再生装置10内のセキュアデコーダ17と、課金データチャージャ25とが、この例では有線の通信路を介して通信を行い、複製/聴取権データが課金データチャージャ25からセキュアデコーダ17内のメモリに対して転送される。複製/聴取権データは、例えばデータ記録再生装置10の、記録(複製)可能回数又は記録(複製)可能時間/再生可能回数情報又は再生可能時間に対応している。

データ記録再生装置10のセキュアデコーダ17から課金データチャージャ25に対して、データ記録再生装置10の複製/再生履歴情報(複製/再生ログ)が伝送される。複製ログには、複製したデータの識別子及び/又は又は複製の条件を含む。具体的には、複製した音楽コンテンツの識別子、種類、複製回数、複製時間等の情報を含んでいる。

再生ログは、復号したデジタルデータの識別子及び/又は復号の条件を含む。具体的には、聴取した音楽コンテンツの識別子、種類、再生回数、再生時間等の情報を含んでいる。この例では、再生時には、復号に対して課金される。

複製/再生ログには、ユーザ端末の所有者、ユーザデバイスとしてのデータ記録再生装置10の識別子等の課金対象者を特定するための識別子が含まれている。セキュアデコーダ17と課金データチャージャ25との間では、前述の図2に示した暗号処理部112と暗号処理及び制御部21を利用して、必要に応じて認証を行い、暗号処理部112と制御部21との間で認証が成立すると、暗号化された複製/聴取権データ及び複製/再生ログの伝送がなされる。

複製/聴取権データは、決済センター203から通信路206例えば電話回線を介して課金データチャージャ25に渡される。又は、決済センター203から通信路207を介して販売端末205に渡された複製/聴取権データが通信路208を介して課金データチャージャ25に渡される。この場合にも、セキュリティの確保のために、例えば決済センター203と課金データチャージャ25との間で認証と暗号化とがなされる。

課金データチャージャ25に吸い上げられた複製/再生ログは、通信路206を介して決済センター203に送られる。又は、複製/再生ログは、通信路20

8を介して販売端末205に渡される。販売端末205は、通信路207を介して決済センター203から聴取権データを受け取ると共に、再生ログを決済センター203へ送る。さらに、販売端末205は、入手した聴取権データの代金を決済センター203に支払う。通信路207は、電話回線、インターネット等である。

決済センター203と聴取権データチャージャ25との間では、通信路206を介して複製／聴取権データ及び複製／再生ログの送受信がなされる。この場合にも、セキュリティの確保のために、決済センター203と聴取権データチャージャ25との間で認証とデータ授受の際の暗号化とがなされる。聴取権データの決済に関して、銀行、クレジットカード会社204が存在している。銀行、クレジットカード会社204は、予め登録してあるユーザの銀行口座から決済センター203の依頼に基づいて、課金データチャージャ25に書き込んだ複製／聴取権データに相当する金額を引き落とす。

さらに、決済センター203は、レコード会社201から複製／聴取権データに関するサービスの管理の委託を受ける。決済センター203は、レコード会社201に対して複製／聴取権データに関する技術の提供を行い、さらに、楽曲聴取料を支払う。レコード会社201は、著作権管理機構202に対して著作権の登録を行うことによって、著作権の管理を依頼し、著作権管理機構202から著作権料を受け取る。

なお、通信路208の代わりに、ICカードを利用することもできる。すなわち、課金データチャージャ25及び販売端末205は、ICカードの書込み／読出し部を備えるようにする。ICカードを課金データチャージャ25に差し込んだ時には、課金データチャージャ25は、ICカードに格納されている複製／聴取権データを吸い上げるとともに、複製／再生ログのデータをICカードに書き込むようにする。ICカードの複製／聴取権データは、課金データチャージャ25に吸い上げられると、クリアされて零となる。

販売端末205にICカードを差し込んだ時には、ユーザが必要な複製／聴取権データの度数を設定することにより、当該設定された複製／聴取権データがICカードに書き込まれる。このとき、同時に、ICカードに格納されていた複製

／再生ログが販売端末 205 に吸い上げられ、IC カードの複製／再生ログは、クリアされる。

以上説明したような課金システムにおいて、この実施の形態では、記録ルール又は再生ルールとして、課金処理が必要な処理が設定されていた場合には、データ記録再生装置 10 のセキュアデコーダ 17 において、複製又は再生についての課金処理が実行される。

図 12 は、複製記録の際のステップ S 48 において、記録ルールが課金を伴う記録と設定されている場合におけるステップ S 49 での処理のフローチャートである。

すなわち、まず、セキュアデコーダ 17 のメモリの複製権データの度数の残を調べ、課金処理可能であるか否か判別する（ステップ S 81）。ステップ S 81 で課金処理が可能であると判別されたときには、記録（複製）を実行する（ステップ S 82）。記録が終了したことを確認すると（ステップ S 83）、セキュアデコーダ 17 のメモリの複製権データの度数を減じる（ステップ S 84）。そして、複製ログとして、例えば複製した音楽コンテンツの識別子、種類、複製回数、複製時間等の情報をそのメモリに記憶し（ステップ S 85）、課金処理を終了する。

一方、セキュアデコーダ 17 のメモリの複製権データの度数の残が無く、ステップ S 81 で課金処理が不可と判別された場合には、複製権データの度数残が無い旨のメッセージを表示するなどしてユーザに知らせる（ステップ S 86）。複製権データが追加されたか否か判別し（ステップ S 87）、追加されたときには、ステップ S 82 に進み、記録を実行して、上述のステップ S 83 以降の処理を行う。ステップ S 87 で複製権データの追加が無かったと判別されたときには、記録不可と判定して（ステップ S 88）、この課金処理ルーチンを終了する。

図 13 は、再生の際のステップ S 73 において、再生ルールが課金を伴う再生と設定されている場合におけるステップ S 74 での処理のフローチャートである。

すなわち、まず、セキュアデコーダ 17 のメモリの聴取権データの度数の残を調べ、課金処理可能であるか否か判別する（ステップ S 91）。ステップ S 91 で課金処理が可能であると判別されたときには、再生データの暗号を解除する復

号を実行する（ステップS 9 2）。復号が完了したことを確認すると（ステップS 9 3）、セキュアデコーダ1 7のメモリの聴取権データの度数を減じる（ステップS 9 4）。再生ログとして、例えば再生した音楽コンテンツの識別子、種類、再生回数、再生時間等の情報をそのメモリに記憶し（ステップS 9 5）、課金処理を終了する。

一方、セキュアデコーダ1 7のメモリの聴取権データの度数の残が無く、ステップS 9 1で課金処理が不可と判定された場合には、聴取権データの度数残が無い旨のメッセージを表示するなどしてユーザに知らせる（ステップS 9 6）。聴取権データが追加されたか否か判別し（ステップS 9 7）、ステップS 9 7で追加されたと判定されたときには、ステップS 9 2に進み、復号を実行して、上述のステップS 9 3以降の処理を行う。ステップS 9 7で聴取権データの追加が無かったときには、再生不可として再生動作を禁止し（ステップS 9 8）、この課金処理ルーチンを終了する。

なお、ステップS 9 8では、完全に再生不可とするのではなく、さわりの部分やさびの部分のみの再生を可とするようにしてもよい。

〔その他の実施の形態〕

上述の実施の形態においては、再生時には、ユーザIDモジュールは、データ記録再生装置あるいはパーソナルコンピュータには接続しなくても再生可能としたが、再生時にも、ユーザIDモジュールを接続しなければ、再生できないような仕組みとしてもよい。すなわち、不揮発性メモリ1 4を設けずに、再生時にもユーザIDモジュールの接続を必須として、ユーザIDモジュールからのユーザIDと、再生データから検出したユーザIDとを照合するようにしてもよい。

再生処理としては、上述の実施の形態と同様とするも、例えば、再生前に、データ記録再生装置に対するユーザIDモジュールの接続を確認し、不揮発性メモリ1 4に記憶されているユーザIDと、使用者を示すユーザIDモジュールからのユーザIDとの照合を行って、使用者を確認してから、上述の再生動作を行うようにすることもできる。

上述の実施の形態の場合においては、記録時には、ユーザIDモジュールの証確認は行いが、ユーザIDを用いた確認は行っていない。しかし、記録時に、ユ

ーザIDモジュールをデータ記録再生装置に接続したときに、ユーザIDを用いたユーザIDモジュールの認証確認を行うようにしてもよい。

上述の実施の形態は、記録再生装置の場合であるが、記録専用装置や、再生専用装置にも、この発明は適用可能である。その場合、ユーザIDモジュールは、上述の第1及び第2の実施の形態と同様の形態では、記録専用装置に付属すべきものである。再生専用装置の場合には、再生専用装置には、ユーザIDを、その不揮発性メモリに一旦登録すれば、再生時には、再生装置にユーザIDモジュールを接続しておく必要はない。

もともと、これらの実施の形態にも、上述のその他の実施の形態を適用することも、勿論できる。

なお、上述の第1及び第2の実施の形態におけるユーザID登録は、データ記録再生装置のうちの再生装置部分に対するユーザ登録である。前述の第1及び第2の実施の形態では、記録装置に対しては、ユーザIDモジュールを必ず接続して、そのユーザIDを記録するようにするので、記録装置部分のみを考え場合には、ユーザIDを登録する必要はない。

しかし、記録専用装置や記録再生装置の記録装置部分の機能を特定の使用者専用とする場合には、ユーザIDモジュールを用いて、ユーザIDを登録して不揮発性メモリに記憶しておき、記録の際にユーザIDが一致したときに、記録が可能となるようにする仕組みとすることもできる。

上述の実施の形態では、ユーザIDとしては、ユーザ名やモジュールIDを用いるようにしたが、使用者の指紋や声紋、あるいは脈などの各個人に固有の生体情報を使用するようにしても良い。その場合に、再生装置では、不揮発性メモリに記憶されている生体情報のユーザIDと再生データから検出した生体情報のユーザIDとを照合するようにしても良いが、不揮発性メモリを設けずに、再生データから検出した生体情報のユーザIDと、指紋や声紋、あるいは脈などの生体情報入力手段から入力された生体情報のユーザIDとを照合するようにすることもできる。この場合に、生体情報入力手段は、ユーザIDモジュールを用いることができる。

なお、音楽会社などから提供される読み出し専用形式のディスクのように、市

販される記録媒体は、「オリジナル」として扱うこととし、前述したように、所有者は無しとされる。ただし、この「オリジナル」から複製が行われた場合には、その複製には、前述したように、ユーザIDが記録され、所有者が特定されることになる。

上述の実施の形態では、ユーザ名については、特に制限を付けなかったが、ユーザ名は個人名であっても、ファミリー名のようなグループ名であってもよい。要するに、著作権法上「個人の使用の範囲内」と認められるような範囲で共有が可能である。

1台の記録ないし再生装置に、複数個のユーザIDを登録することができるようにして、前記1台の装置を、前記複数個のユーザIDに対応する複数の使用者で共有するようにすることもできる。

上述の実施の形態では、ユーザIDは、記録データに埋め込むようにしたが、記録データとは別領域に記録するようにしても勿論よい。また、記録データを、コンピュータデータのようにファイル単位に取り扱う場合には、ファイル単位にユーザIDを記録データに付加することができる。

上述の実施の形態では、記録時には、ユーザIDモジュール20をデータ記録再生装置10に接続することを必須としたが、記録時に、ユーザIDモジュール20を接続することなく、データ記録再生装置10の不揮発性メモリ14に蓄えられているユーザID（特にモジュールID）と、記録対象のデータに付随するユーザIDとを比較照合するようにしてもよい。

記録ルールとして、不揮発性メモリ14に記憶されているユーザIDと、記録対象のデータに付随するユーザIDとが一致したときには、ユーザIDモジュール20はデータ記録再生装置10には接続不要という設定を行えるようにしてもよい。

記録対象のデータに付随するユーザIDというときには、記録対象のデータに埋め込まれていることのみを意味するのではなく、上述もしたように、記録媒体のTOCエリアや、その他の記録対象データの記録部分とは別個のエリアから、ユーザIDを取得することも含む。また、インターネットからダウンロードしたデータを記録対象とする場合に、そのダウンロードデータの最初、中間あるいは

最後に、ユーザIDが付加されるような場合も含む。

記録対象のデータは、データ記録再生装置10において記録媒体から再生されたものではなく、アナログ入力とされた、あるいはデジタル入力とされたデータを含むものであることは言うまでもない。その場合に、その入力データは、ディスクから再生された再生データである必要もない。

なお、上述の実施の形態は、記録対象のコンテンツとして、オーディオデータを例にとったが、映像データやプログラム、ゲームのプログラムやデータなど、著作権管理が必要なコンテンツのいずれも、この発明の記録対象である。

記録媒体としては、ディスクに限らず、カード形メモリや、半導体メモリ、ハードディスク装置のハードディスクなどであってもよい。さらに、記録対象となるデータは、前述もしたように、記録媒体から再生されたデータに限られるものではなく、有線電話回線や無線電話回線又はインターネットを通じて送られてくるデータであってもよい。

また、上述の実施の形態は、記録対象のコンテンツとして、オーディオデータを例にとったが、映像データやプログラム、ゲームのプログラムやデータなど、著作権管理が必要なコンテンツのいずれも、この発明の記録対象である。

上述の実施の形態では、ユーザIDは、記録データに埋め込むようにしたが、記録データとは別領域に記録するようにしても勿論よい。また、記録データを、コンピュータデータのようにファイル単位に取り扱う場合には、ファイル単位にユーザIDを記録データに付加することができる。

産業上の利用可能性

本発明によれば、記録時に、登録されたユーザIDを記録データと共に記録し、再生時には、不揮発性メモリ14などに用意されるユーザIDと、記録媒体から読み出されたデータから検出されたユーザIDとを比較して、両者が一致したときに、正常な再生出力を行うようにしたことにより、個人的な利用形態に限って複製を可能にすることができる。

請求の範囲

1. データとともに使用者を特定するための使用者識別データが記録された記録媒体から読み出された上記使用者識別データと上記記録媒体の記録又は再生時に装置から読み出された使用者識別データとを比較し、

上記記録媒体から読み出された使用者識別データと上記装置から読み出された使用者識別データとが一致したときに、上記記録媒体に記録又は再生を行う記録媒体の記録及び／又は再生方法。

2. 上記記録媒体には、更に上記記録媒体の記録又は再生動作を管理するための管理データが記録されており、上記方法は、上記記録媒体から読み出された使用者識別データと上記装置から読み出された使用者識別データとが一致しなかったときには、上記記録媒体から読み出された上記管理データに基づいて上記記録媒体に記録又は再生を行う請求の範囲第1項記載の記録媒体の記録及び／又は再生方法。

3. 上記方法は、上記記録媒体から読み出された使用者識別データと上記装置から読み出された使用者識別データとが一致したときに、上記装置から読み出された使用者識別データを暗号鍵として上記記録媒体に記録するデータに暗号化処理を施して上記記録媒体に記録する請求の範囲第1項記載の記録媒体の記録及び／又は再生方法。

4. 上記方法は、上記装置から読み出された使用者識別データを上記記録媒体に記録するデータに埋め込む請求の範囲第3項記載の記録媒体の記録及び／又は再生方法。

5. 上記方法は、上記装置から読み出された使用者識別データを暗号化して上記記録媒体に記録するデータに埋め込む請求の範囲第3項記載の記録媒体の記録及び／又は再生方法。

6. 上記記録媒体には、更に上記記録媒体の記録又は再生動作を管理するための管理データが記録されており、上記方法は、上記記録媒体から読み出された使用者識別データと上記装置から読み出された使用者識別データとが一致しなかったときには、上記記録媒体から読み出された上記管理データに基づいて上記記録媒

体の再生を行う請求の範囲第1項記載の記録媒体の記録及び／又は再生方法。

7. 上記方法は、上記記録媒体から読み出された使用者識別データと上記装置から読み出された使用者識別データとが一致しなかったときに、上記記録媒体から読み出された使用者識別データが特定の識別データであったときには、上記記録媒体の再生を許可する請求の範囲第6項記載の記録媒体の記録及び／又は再生方法。

8. 上記特定の識別データは、上記記録媒体がオリジナルの記録媒体であることを示す識別データである請求の範囲第7項記載の記録媒体の記録及び／又は再生方法。

9. 上記装置から読み出される使用者識別データは、ユーザによって設定される請求の範囲第1項記載の記録媒体の記録及び／又は再生方法。

10. 上記使用者識別データは、ユーザ名を含むデータである請求の範囲第9項記載の記録媒体の記録及び／又は再生方法。

11. データとともに使用者を特定するための使用者識別データが記録された記録媒体から読み出された上記使用者識別データと上記記録媒体の記録時に装置から読み出された使用者識別データとを比較し、

上記記録媒体から読み出された使用者識別データと上記装置から読み出された使用者識別データとが一致したときに、上記記録媒体に記録を行う記録媒体の記録方法。

12. 上記記録媒体には、更に上記記録媒体の記録動作を管理するための管理データが記録されており、上記方法は、上記記録媒体から読み出された使用者識別データと上記装置から読み出された使用者識別データとが一致しなかったときには、上記記録媒体から読み出された上記管理データに基づいて上記記録媒体の記録を行う請求の範囲第11項記載の記録媒体の記録方法。

13. 上記方法は、上記記録媒体から読み出された使用者識別データと上記装置から読み出された使用者識別データとが一致したときに、上記装置から読み出された使用者識別データを暗号鍵として上記記録媒体に記録するデータに暗号化処理を施して上記記録媒体に記録する請求の範囲第11項記載の記録媒体の記録方法。

14. 上記方法は、上記装置から読み出された使用者識別データを上記記録媒体に記録するデータに埋め込む請求の範囲第13項記載の記録媒体の記録方法。

15. 上記方法は、上記装置から読み出された使用者識別データを暗号化して上記記録媒体に記録するデータに埋め込む請求の範囲第14項記載の記録媒体の記録方法。

16. 上記装置から読み出される使用者識別データは、ユーザによって設定される請求の範囲第11項記載の記録媒体の記録方法。

17. 上記使用者識別データは、ユーザ名を含むデータである請求の範囲第16項記載の記録媒体の記録方法。

18. データとともに使用者を特定するための使用者識別データが記録された記録媒体を走査するヘッド部と、

使用者識別データが記憶されたメモリと、

上記ヘッド部によって上記記録媒体から読み出された使用者識別データと上記メモリから読み出された使用者識別データとを比較し、上記比較結果に基づいて上記記録媒体の記録動作を制御する制御部とを備えている記録媒体の記録装置。

19. 上記制御部は、上記記録媒体から読み出された使用者識別データと上記メモリから読み出された使用者識別データとが一致したときに、上記ヘッド部を制御して上記記録媒体に記録を行う請求の範囲第18項記載の記録媒体の記録装置。

20. 上記メモリは、上記装置に接続される使用者識別データ提供部に設けられている請求の範囲第18項記載の記録媒体の記録装置。

21. 上記制御部は、上記装置に上記提供部が接続されていると判別されたときには上記提供部との間で認証処理を行う請求の範囲第20項記載の記録媒体の記録装置。

22. 上記制御部は、上記認証処理が正しく終了したときには上記提供部に上記メモリから上記使用者識別データを読み出すように指示をする請求の範囲第21項記載の記録媒体の記録装置。

23. 上記メモリから読み出された使用者識別データは暗号化処理が施されて、上記提供部から上記制御部に送信される請求の範囲第22項記載の記録媒体の記録装置。

24. 上記制御部は、上記認証処理が正しく終了できなかったときには上記記録媒体の記録動作を中止する請求の範囲第21項記載の記録媒体の記録装置。

25. 上記制御部は、上記装置に上記提供部が接続されていないと判別されたときには使用者に上記提供部を接続するように告知する請求の範囲第21項記載の記録媒体の記録装置。

26. 上記記録媒体には、更に上記記録媒体の記録動作を管理するための管理データが記録されており、上記制御部は、上記記録媒体から読み出された使用者識別データと上記メモリから読み出された使用者識別データとが一致しなかったときには、上記記録媒体から読み出された上記管理データに基づいて上記記録媒体の記録を行う請求の範囲第19項記載の記録媒体の記録装置。

27. 上記制御部は、上記記録媒体から読み出された使用者識別データと上記メモリから読み出された使用者識別データとが一致したときに、上記装置から読み出された使用者識別データを暗号鍵として上記記録媒体に記録するデータに暗号化処理を施して上記ヘッド部により上記記録媒体に記録する請求の範囲第26項記載の記録媒体の記録装置。

28. 上記制御部は、上記メモリから読み出された使用者識別データを上記記録媒体に記録するデータに埋め込む請求の範囲第27項記載の記録媒体の記録装置。

29. 上記制御部は、上記メモリから読み出された使用者識別データを暗号化して上記記録媒体に記録するデータに埋め込む請求の範囲第28項記載の記録媒体の記録装置。

30. 上記メモリは、ユーザによって設定された使用者識別データが書きこまれる請求の範囲第18項記載の記録媒体の記録装置。

31. 上記メモリに記憶される使用者識別データは、ユーザによって設定される請求の範囲第18項記載の記録媒体の記録装置。

32. 上記使用者識別データは、ユーザ名を含むデータである請求の範囲第31項記載の記録媒体の記録装置。

33. データとともに使用者を特定するための使用者識別データが記録された記録媒体から読み出された上記使用者識別データと上記記録媒体の再生時に装置から読み出された使用者識別データとを比較し、

上記記録媒体から読み出された使用者識別データと上記装置から読み出された使用者識別データとが一致したときに、上記記録媒体の再生を行う記録媒体の再生方法。

34. 上記記録媒体には、更に上記記録媒体の再生動作を管理するための管理データが記録されており、上記方法は、上記記録媒体から読み出された使用者識別データと上記装置から読み出された使用者識別データとが一致しなかったときには、上記記録媒体から読み出された上記管理データに基づいて上記記録媒体の再生を行う請求の範囲第33項記載の記録媒体の再生方法。

35. 上記方法は、上記記録媒体から読み出された使用者識別データと上記装置から読み出された使用者識別データとが一致しなかったときに、上記記録媒体から読み出された使用者識別データが特定の識別データであったときには、上記記録媒体の再生を許可する請求の範囲第34項記載の記録媒体の再生方法。

36. 上記特定の識別データは、上記記録媒体がオリジナルの記録媒体であることを示す識別データである請求の範囲第35項記載の記録媒体の再生方法。

37. 上記記録媒体には暗号化処理が施されたデータが記録されており、上記方法は上記記録媒体から読み出された使用者識別データと上記装置から読み出された使用者識別データとが一致したときには、上記記録媒体から読み出されたデータに施されている暗号処理を上記使用者識別データを用いて復号処理を行う請求の範囲第33項記載の記録媒体の再生方法。

38. 上記装置から読み出される使用者識別データは、ユーザによって設定される請求の範囲第33項記載の記録媒体の再生方法。

39. 上記使用者識別データは、ユーザ名を含むデータである請求の範囲第38項記載の記録媒体の再生方法。

40. 暗号化処理が施されたデータとともに少なくとも使用者を特定するための使用者識別データと再生管理データが記録された記録媒体を走査するヘッド部と、使用者識別データが記憶されたメモリと、

上記ヘッド部によって上記記録媒体から読み出された使用者識別データと上記メモリから読み出された使用者識別データとを比較し、上記比較結果に基づいて上記記録媒体の再生動作を制御する制御部とを備えている記録媒体の再生装置。

41. 上記制御部は、上記記録媒体から読み出された使用者識別データと上記メモリから読み出された使用者識別データとが一致したときに、上記記録媒体の再生を行う請求の範囲第40項記載の記録媒体の再生装置。

42. 上記制御部は、上記記録媒体から読み出された使用者識別データと上記メモリから読み出された使用者識別データとが一致したときには、上記ヘッド部によって上記記録媒体から読み出されたデータに施されている暗号化処理を上記使用者識別データを用いて復号する請求の範囲第41項記載の記録媒体の再生装置。

43. 上記制御部は、上記ヘッド部によって上記記録媒体から読み出された使用者識別データが検出できなかったときには、上記記録媒体から読み出された上記再生管理データに基づいて上記記録媒体の再生動作を制御する請求の範囲第42項記載の記録媒体の再生装置。

44. 上記メモリは、上記装置に接続される使用者識別データ提供部に設けられている請求の範囲第40項記載の記録媒体の再生装置。

45. 上記制御部は、上記装置に上記提供部が接続されていると判別されたときには上記提供部との間で認証処理を行う請求の範囲第40項記載の記録媒体の再生装置。

46. 上記制御部は、上記認証処理が正しく終了したときには上記提供部に上記メモリから上記使用者識別データを読み出すように指示をする請求の範囲第45項記載の記録媒体の再生装置。

47. 上記メモリから読み出された使用者識別データは暗号化処理が施されて、上記提供部から上記制御部に送信される請求の範囲第46項記載の記録媒体の再生装置。

48. 上記制御部は、上記認証処理が正しく終了できなかったときには上記記録媒体の記録動作を中止する請求の範囲第45項記載の記録媒体の再生装置。

49. 上記制御部は、上記装置に上記提供部が接続されていないと判別されたときには使用者に上記制御部を接続するように告知する請求の範囲第40項記載の記録媒体の再生装置。

50. 上記制御部は、上記記録媒体から読み出された使用者識別データと上記メモリから読み出された使用者識別データとが一致しなかったときに、上記記録媒

体から読み出された使用者識別データが特定の識別データであったときには、上記記録媒体の再生を許可する請求の範囲第41項記載の記録媒体の再生装置。

51. 上記特定の識別データは、上記記録媒体がオリジナルの記録媒体であることを示す識別データである請求の範囲第50項記載の記録媒体の再生装置。

52. 上記メモリには、使用者によって設定された上記使用者識別データが書きこまれる請求の範囲第50項記載の記録媒体の再生装置。

53. 上記装置から読み出される使用者識別データは、ユーザによって設定される請求の範囲第40項記載の記録媒体の再生装置。

54. 上記使用者識別データは、ユーザ名を含むデータである請求の範囲第53項記載の記録媒体の再生装置。

55. 使用者を特定するための使用者識別データが少なくとも埋めこまれたデータから読み出された上記使用者識別データと上記データの複製動作を行う際に装置から読み出された使用者識別データとを比較し、

上記データから抽出された使用者識別データと上記装置から読み出された使用者識別データとが一致したときに、上記データの出力制御を行うデータの複製制御方法。

56. 上記データには、更に上記データの複製動作を管理するための管理データを含んでおり、上記方法は、上記データから抽出された使用者識別データと上記装置から読み出された使用者識別データとが一致しなかったときには、上記管理データに基づいて上記データの複製動作を制御する請求の範囲第55項記載のデータの複製制御方法。

57. 上記方法は、上記データから抽出された使用者識別データと上記装置から読み出された使用者識別データとが一致したときに、上記装置から読み出された使用者識別データを暗号鍵として上記識別データに暗号化処理を施して出力する請求の範囲第56項記載のデータの複製制御方法。

58. 上記方法は、上記装置から読み出された使用者識別データを上記データに埋め込む請求の範囲第57項記載のデータの複製制御方法。

59. 上記方法は、上記装置から読み出された使用者識別データを暗号化して上記データに埋め込む請求の範囲第57項記載のデータの複製制御方法。

60. 上記方法は、上記管理データが上記データの複製を行うにあたって課金処理が必要であることを示しているときには、課金処理が可能であるか否かを判別し、上記判別結果が課金処理可能であることを示しているときに複製を実行する請求の範囲第56項記載のデータの複製制御方法。

61. 上記方法は、上記課金処理は複製可能回数を示す度数を減算することによって行われる請求の範囲第60項記載のデータの複製制御方法。

62. 上記方法は、上記課金処理が不可能であると判別であると判別されたときで、上記度数の加算が行われなかったときには複製動作を停止させる請求の範囲第61項記載のデータの複製制御方法。

63. 上記装置から読み出される使用者識別データは、ユーザによって設定される請求の範囲第55項記載のデータの複製制御方法。

64. 上記使用者識別データは、ユーザ名を含むデータである請求の範囲第63項記載のデータの複製制御方法。

65. 少なくとも使用者を特定するための使用者識別データが埋めこまれたデータから抽出された上記使用者識別データと上記データの再生時に装置から読み出された使用者識別データを比較し、

上記データから抽出された使用者識別データと上記装置から読み出された使用者識別データとが一致したときに、上記データの再生を行うデータの再生方法。

66. 上記データには、更に上記データの再生動作を管理するための管理データが記録されており、上記方法は、上記データから抽出された使用者識別データと上記装置から読み出され使用者識別データとが一致しなかったときには、上記管理データに基づいて上記データの再生を行う請求の範囲第65項記載のデータの再生方法。

67. 上記方法は、上記データから使用者識別データが検出できなかったときには、上記再生管理データに基づいて上記データの再生動作を制御する請求の範囲第66項記載のデータの再生方法。

68. 上記方法は、上記データから抽出された使用者識別データと上記装置から読み出された使用者識別データとが一致しなかったときに、上記データから抽出された使用者識別データが特定の識別データであったときには、上記データの再

生を許可する請求の範囲の66項記載のデータの再生方法。

69. 上記特定の識別データは、上記記録媒体がオリジナルの記録媒体であることを示す識別データである請求の範囲第68項記載のデータの再生方法。

70. 上記方法は、上記管理データが上記データの再生を行うにあたって課金処理が必要であることを示しているときには、課金処理が可能であるか否かを判別し、上記判別結果が課金処理可能であることを示しているときに上記データの再生を実行する請求の範囲第66項記載のデータの再生方法。

71. 上記方法は、上記課金処理は再生可能回数を示す度数を減算することによって行われる請求の範囲第70記載のデータの再生方法。

72. 上記方法は、上記課金処理が不可能であると判別であると判別されたときで、上記度数の加算が行われなかったときには再生動作を禁止する請求の範囲第71項記載のデータの再生方法。

73. 上記データには暗号化処理が施されたデータが記録されており、上記方法は上記データから抽出された使用者識別データと上記装置から読み出された使用者識別データとが一致したときには、上記抽出されたデータに施されている暗号処理を上記使用者識別データを用いて復号処理を行う請求の範囲第65項記載のデータの再生方法。

74. 上記装置から読み出される使用者識別データは、ユーザによって設定される請求の範囲第65項記載のデータの再生方法。

75. 上記使用者識別データは、ユーザ名を含むデータである請求の範囲第74項記載のデータ再生方法。

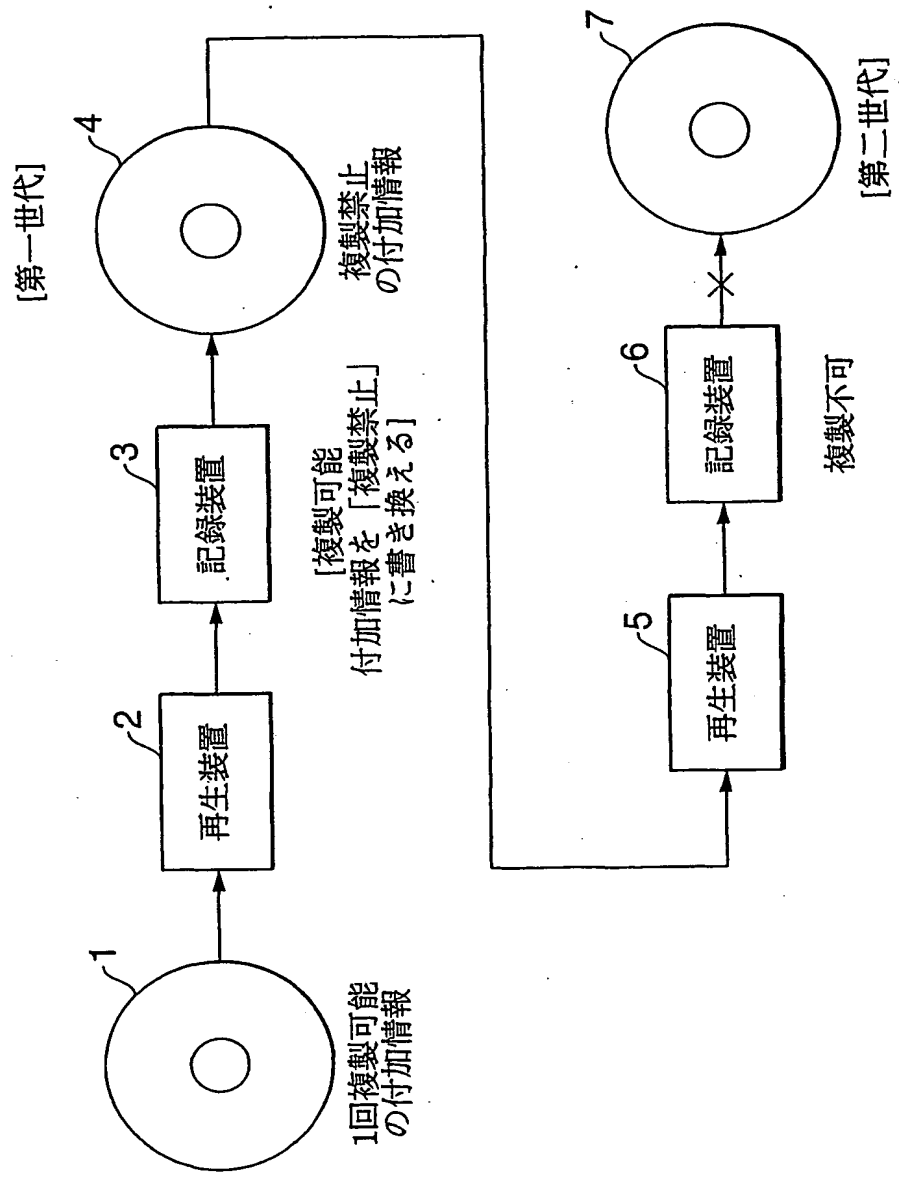


FIG.1

2/13

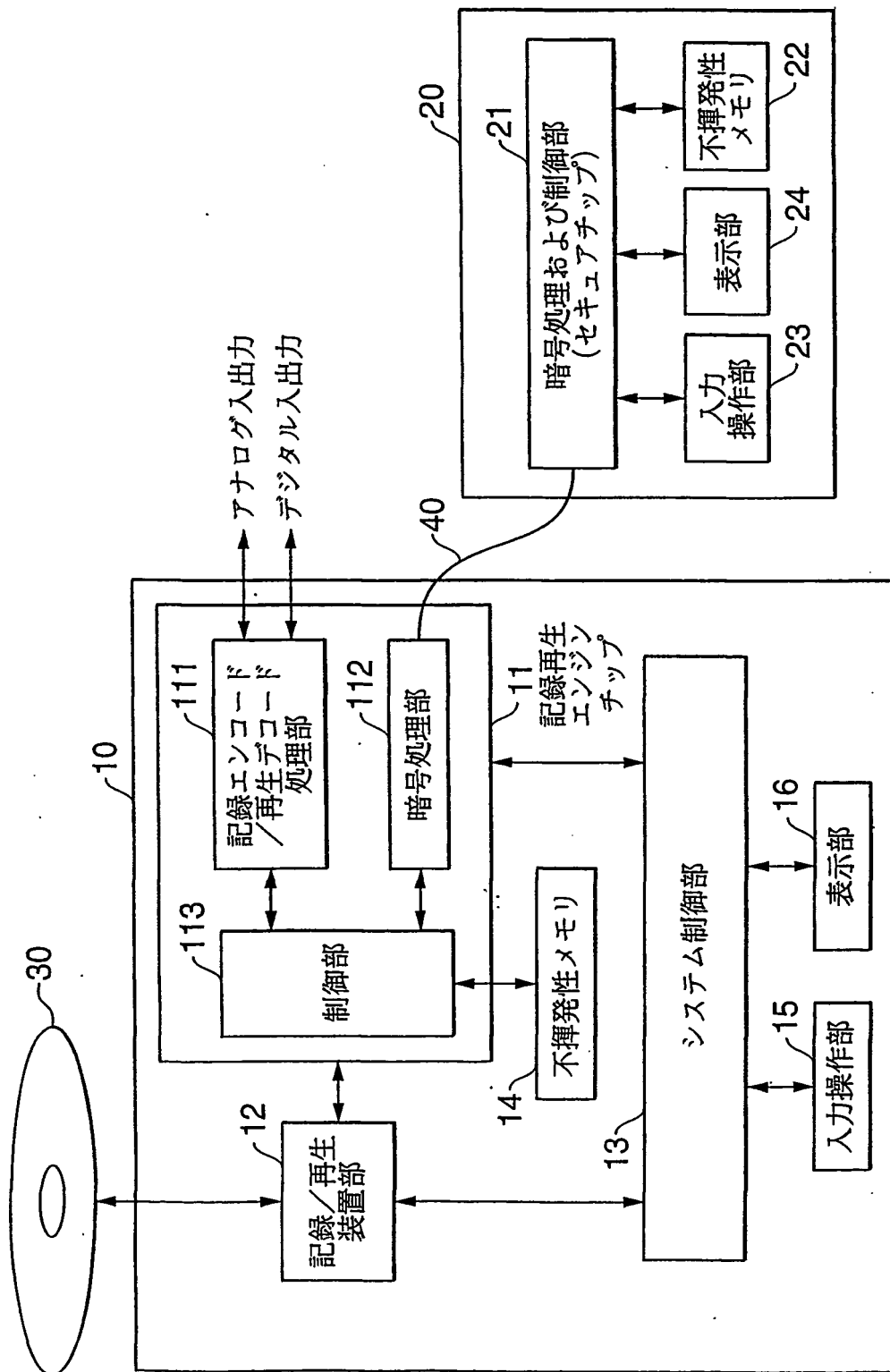


FIG. 2

3/13

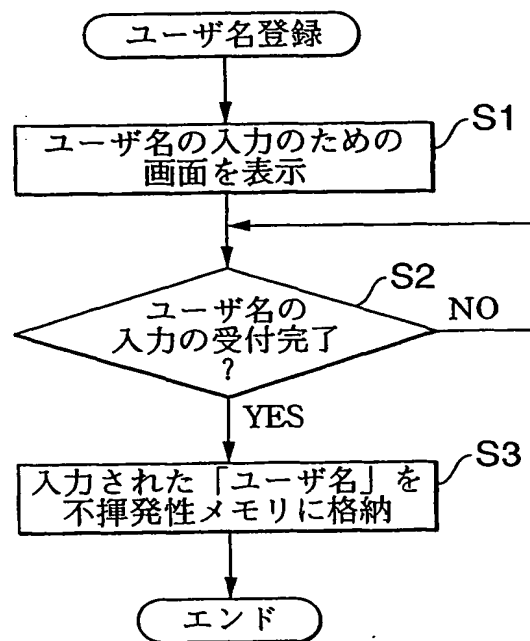


FIG.3

4/13

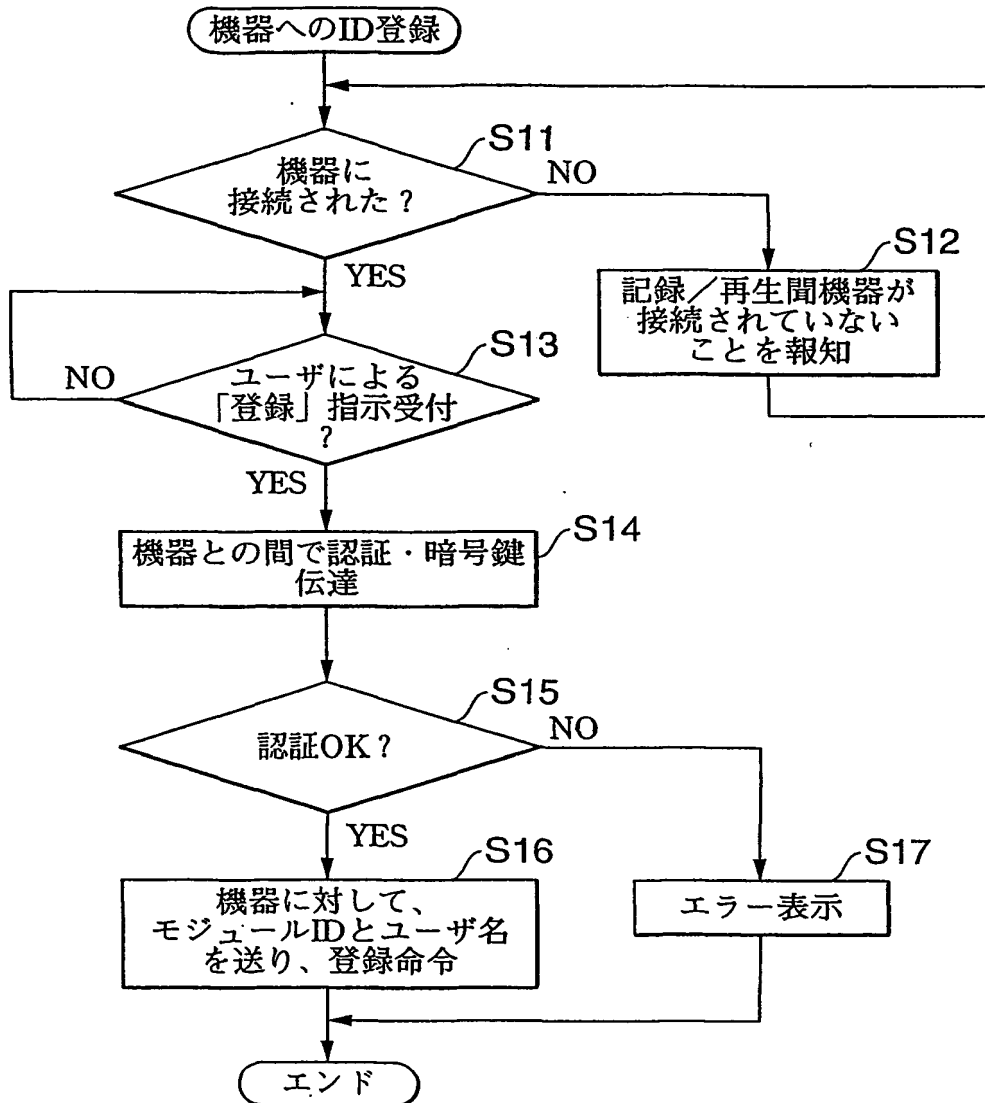


FIG.4

5/13

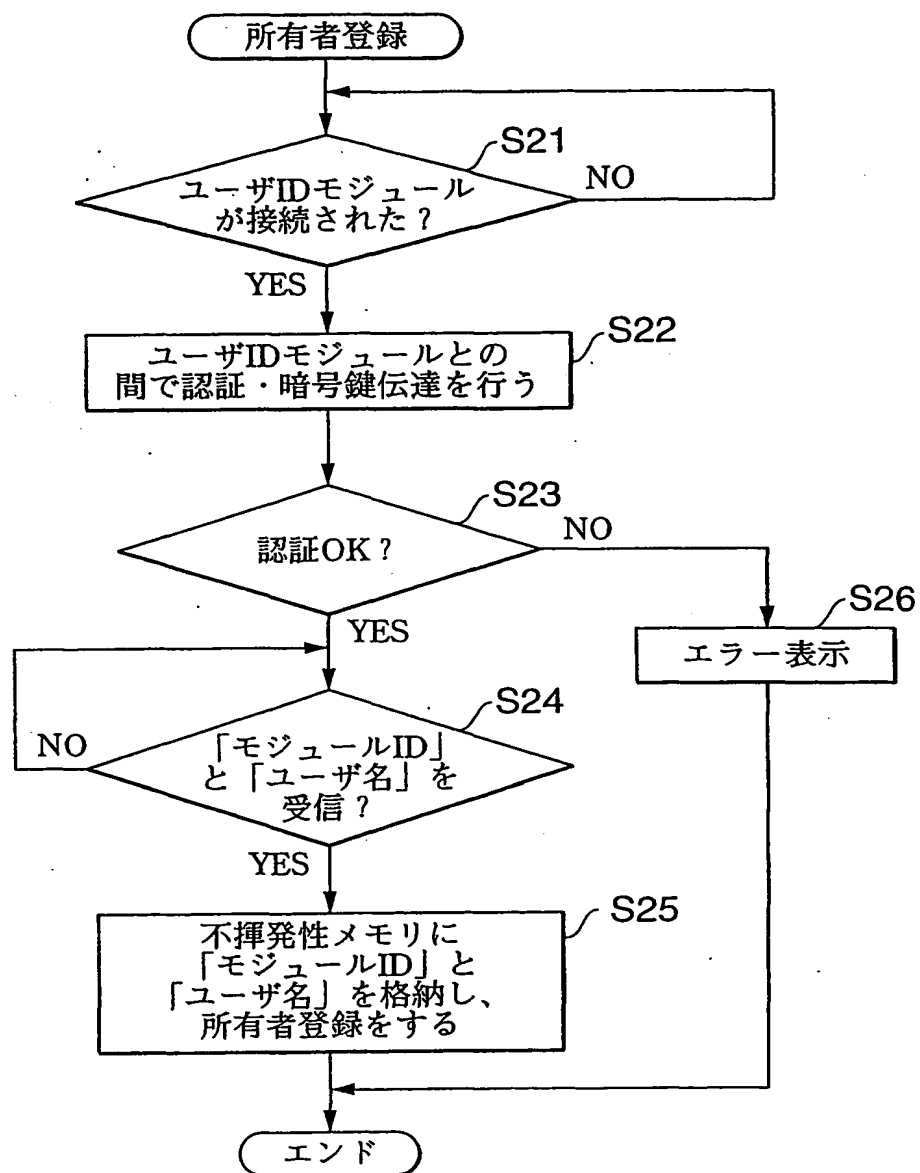


FIG.5

6/13

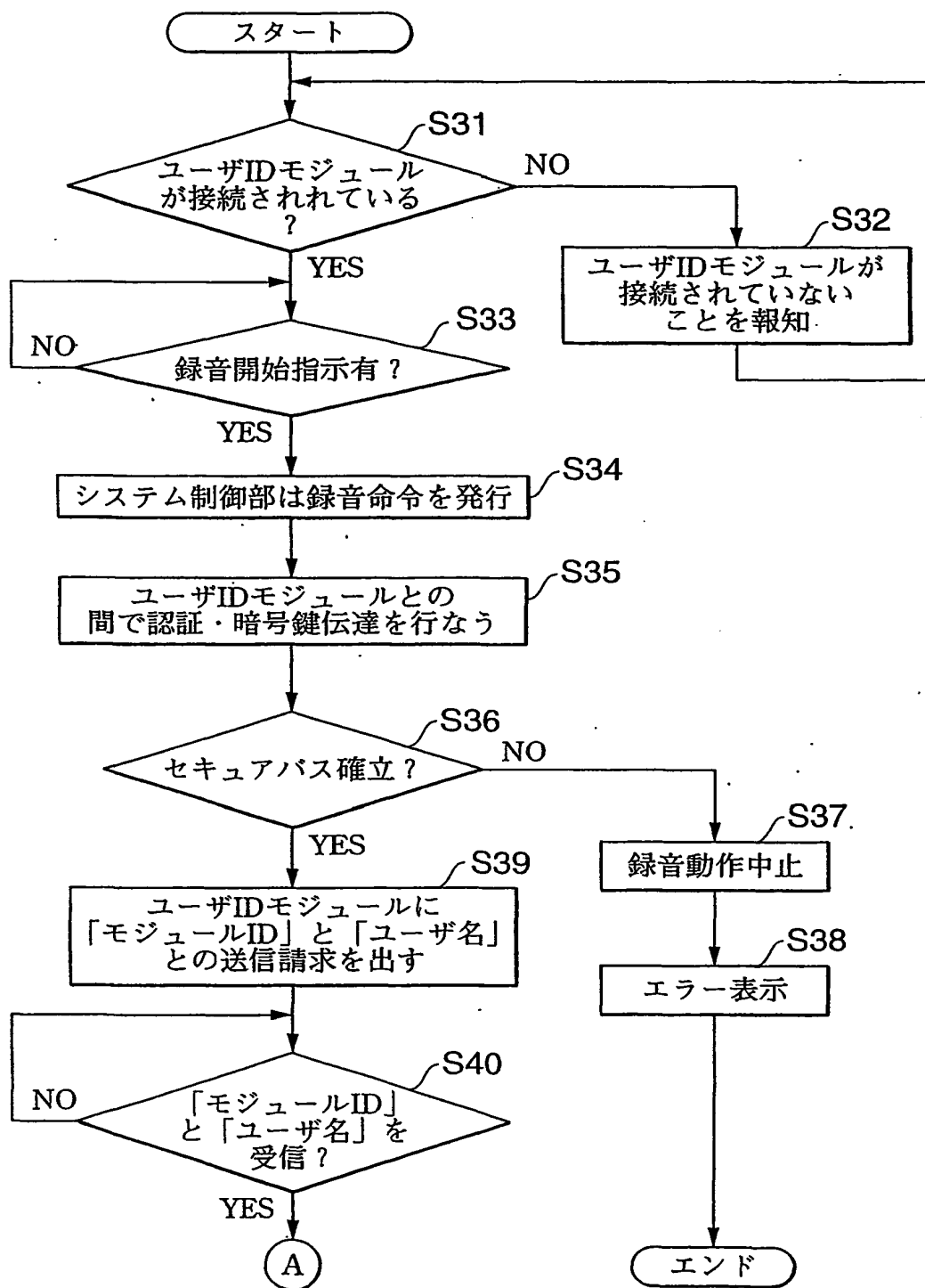


FIG.6

7/13

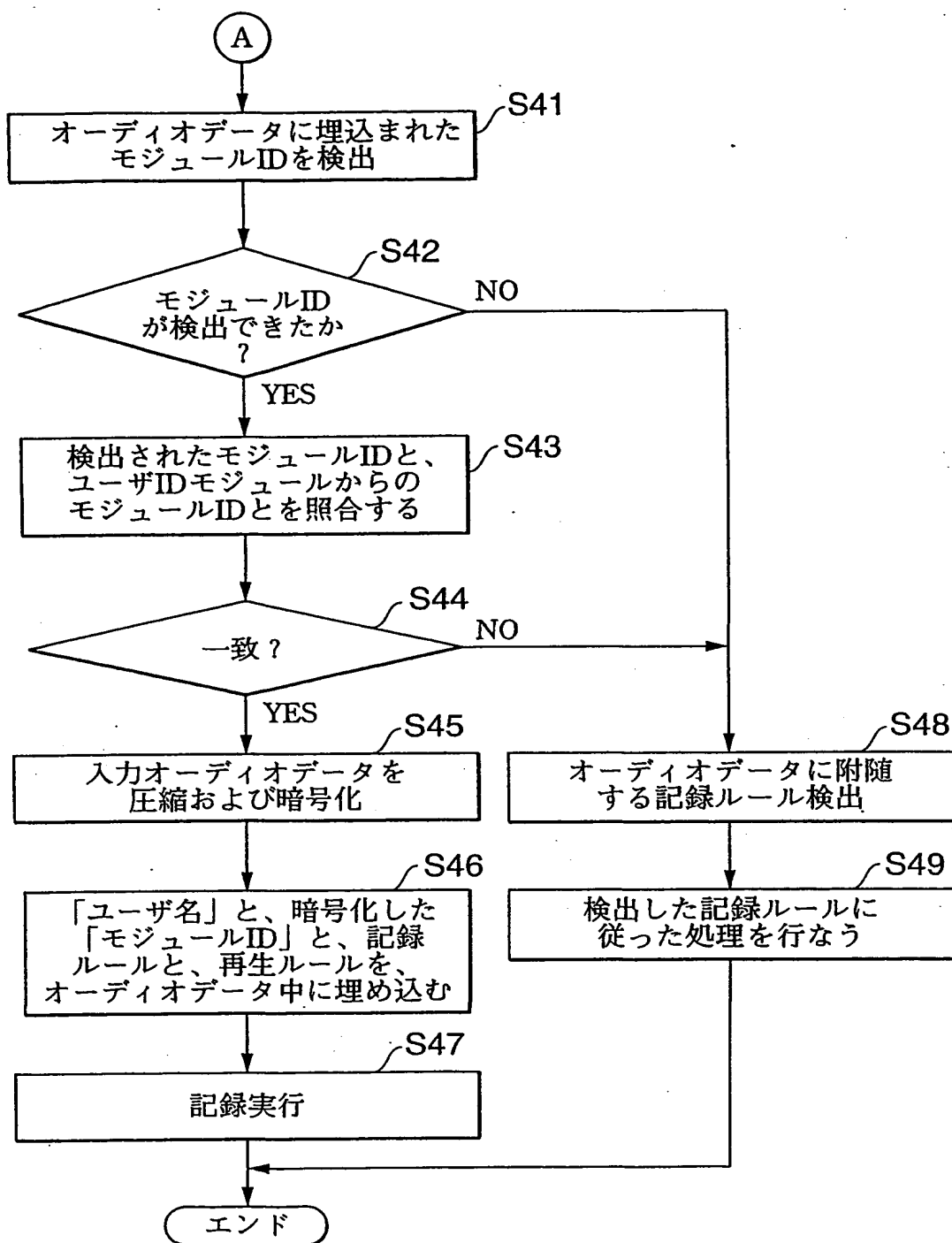


FIG.7

8/13

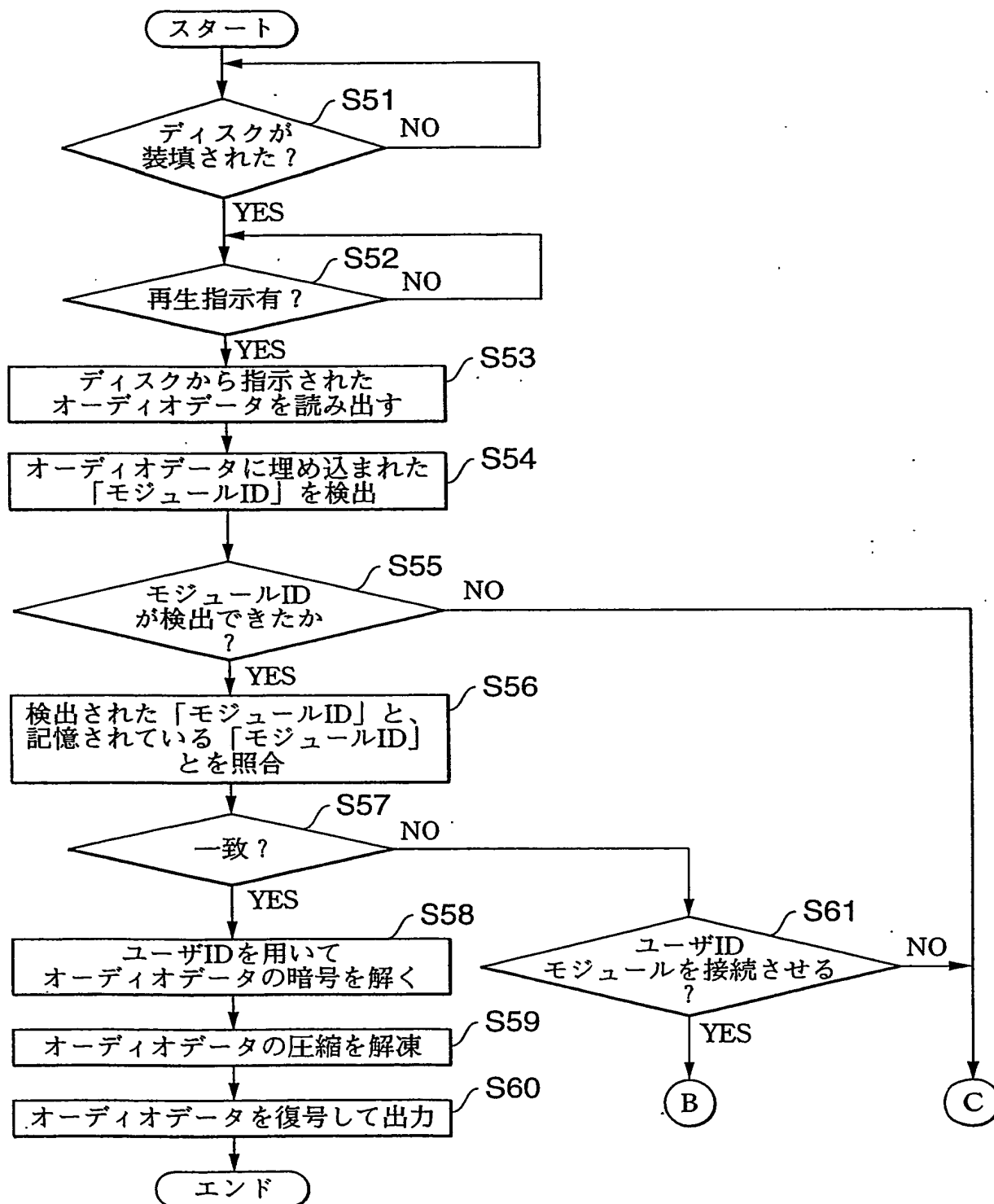


FIG.8

9/13

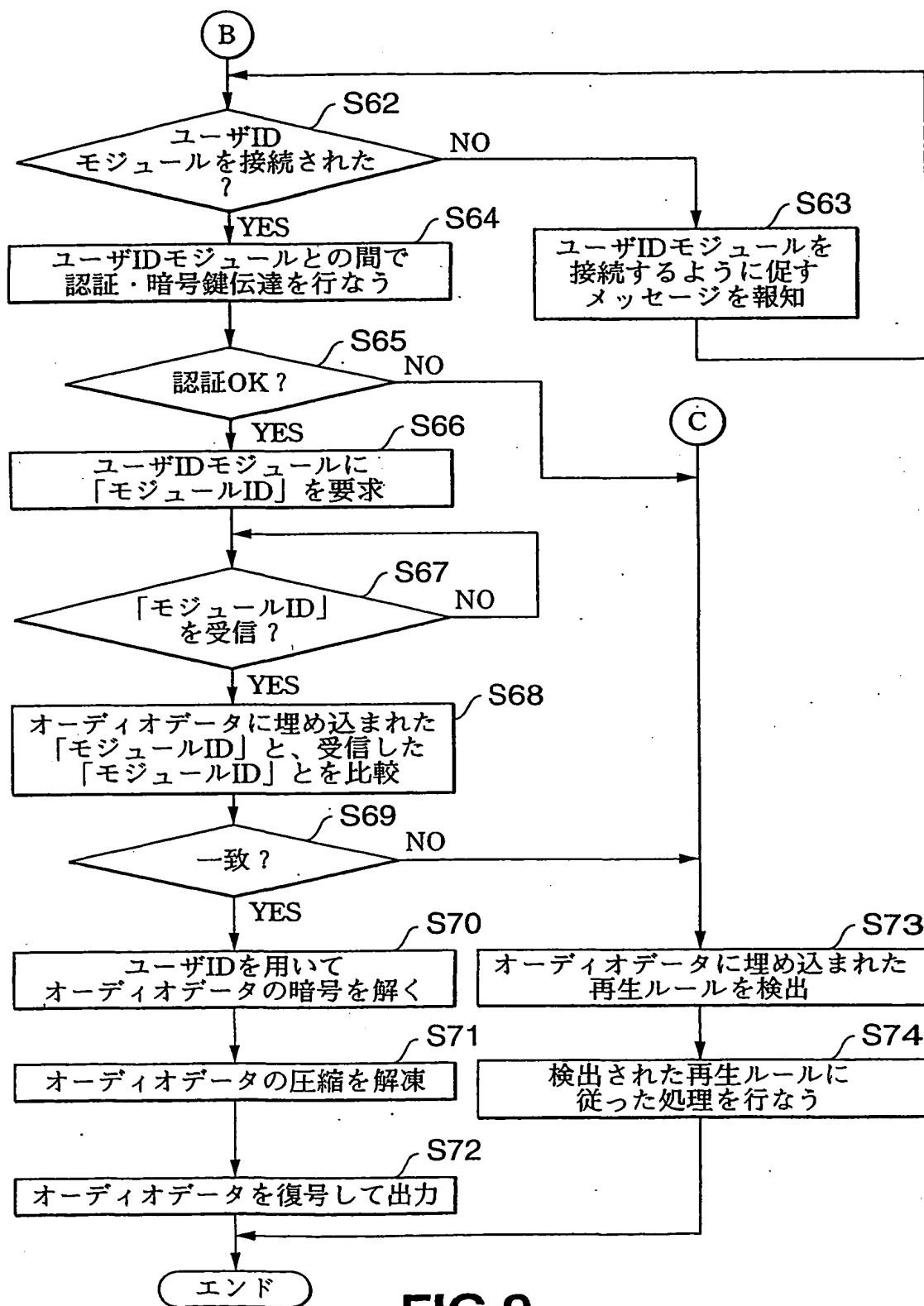


FIG.9

10/13

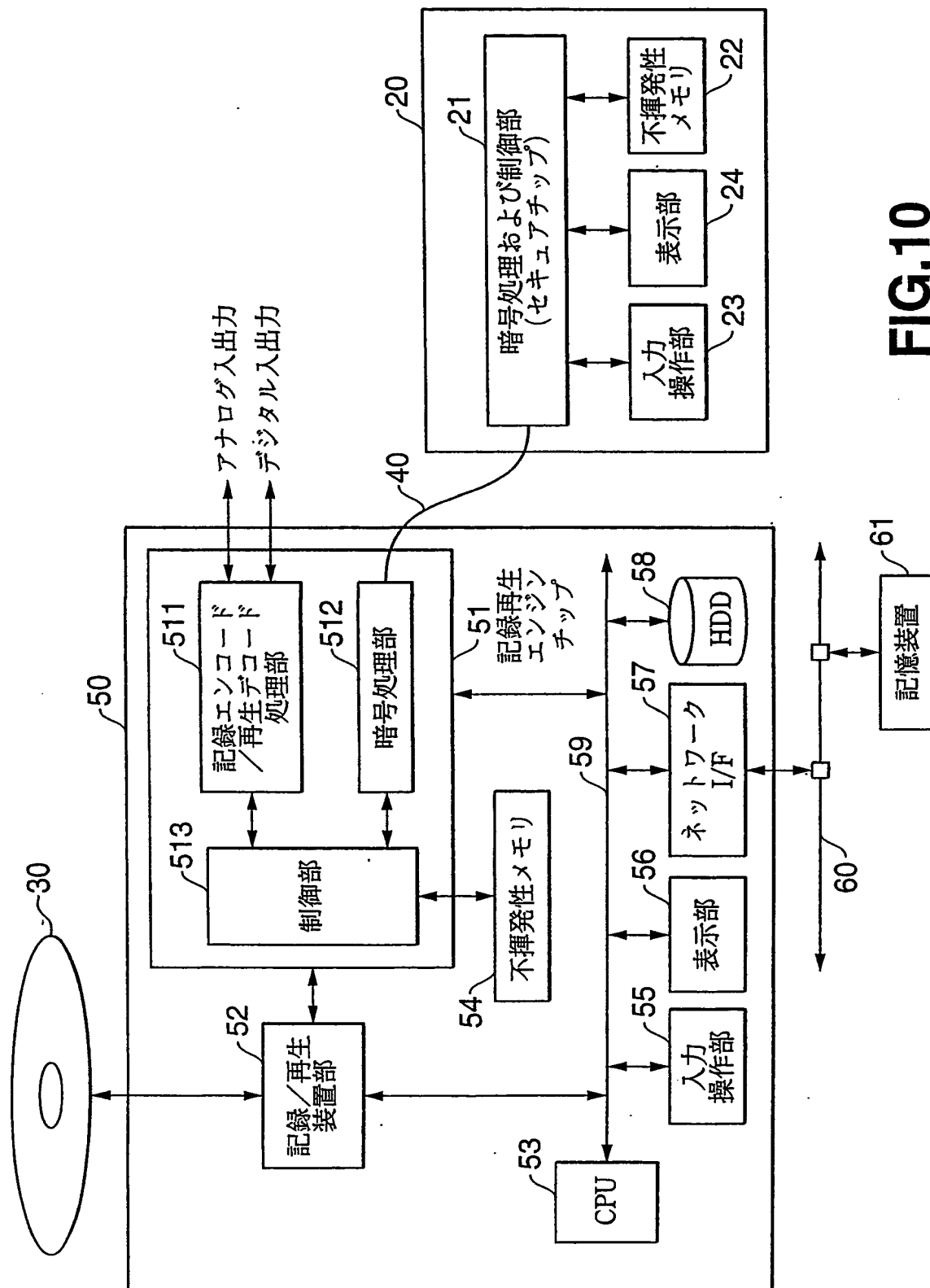


FIG.10

11/13

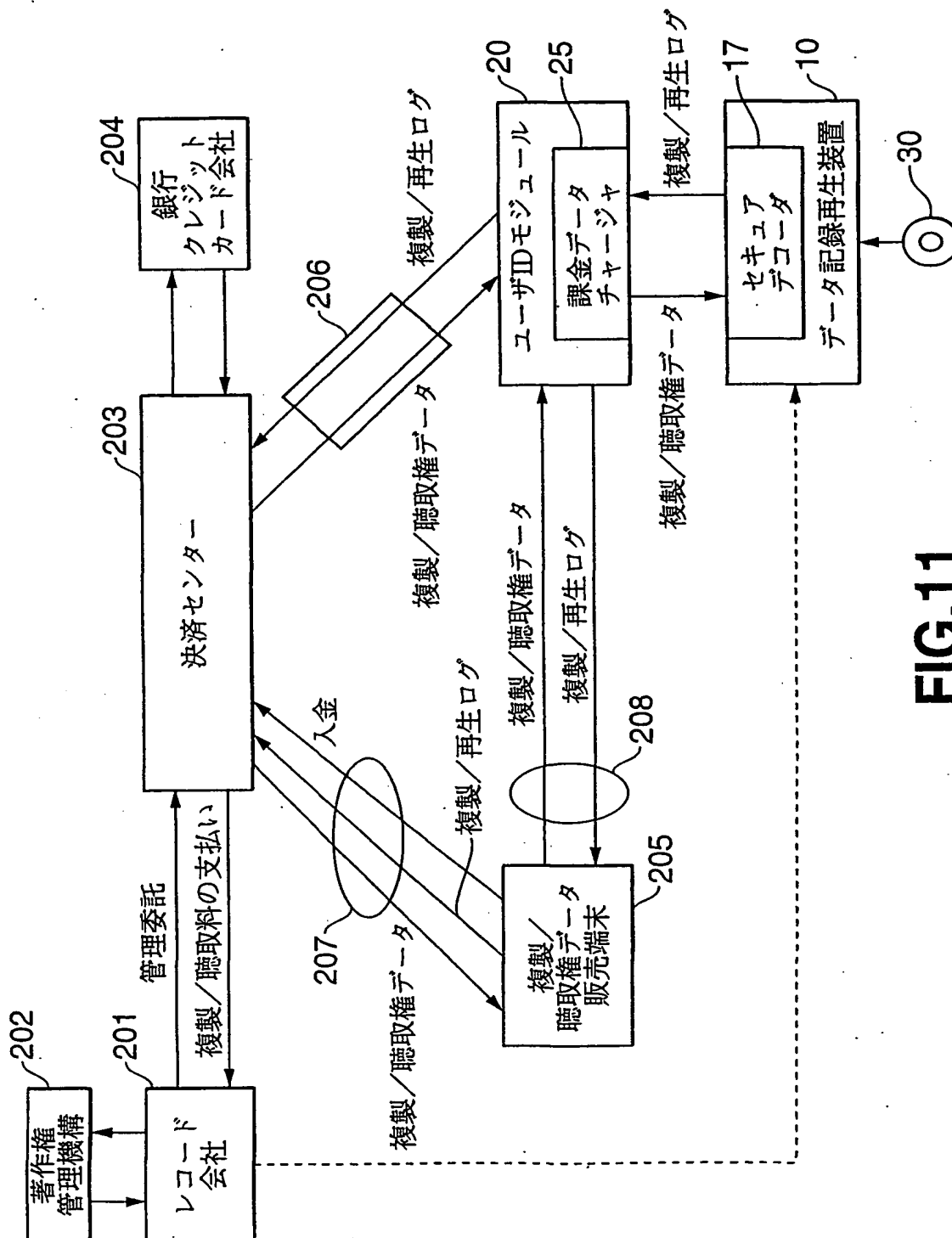


FIG.11

12/13

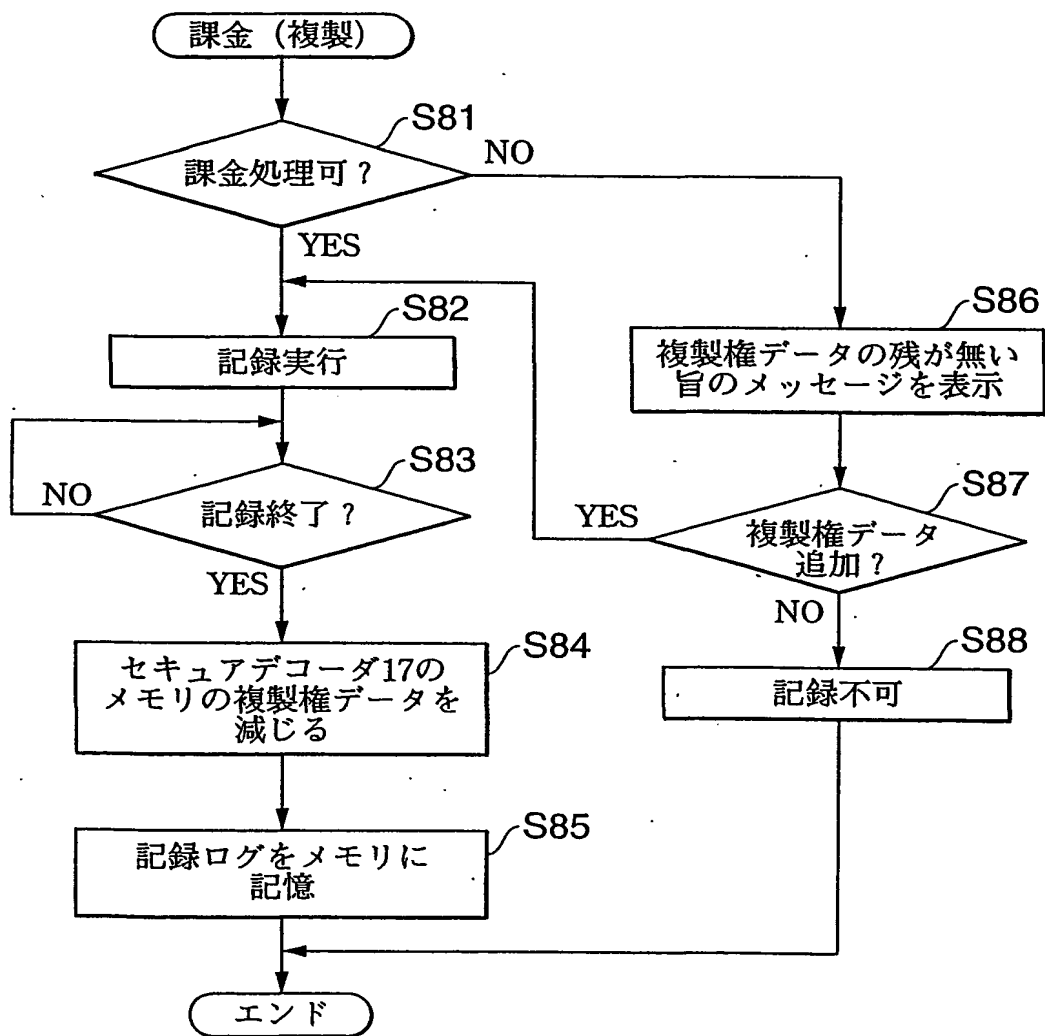


FIG.12

13/13

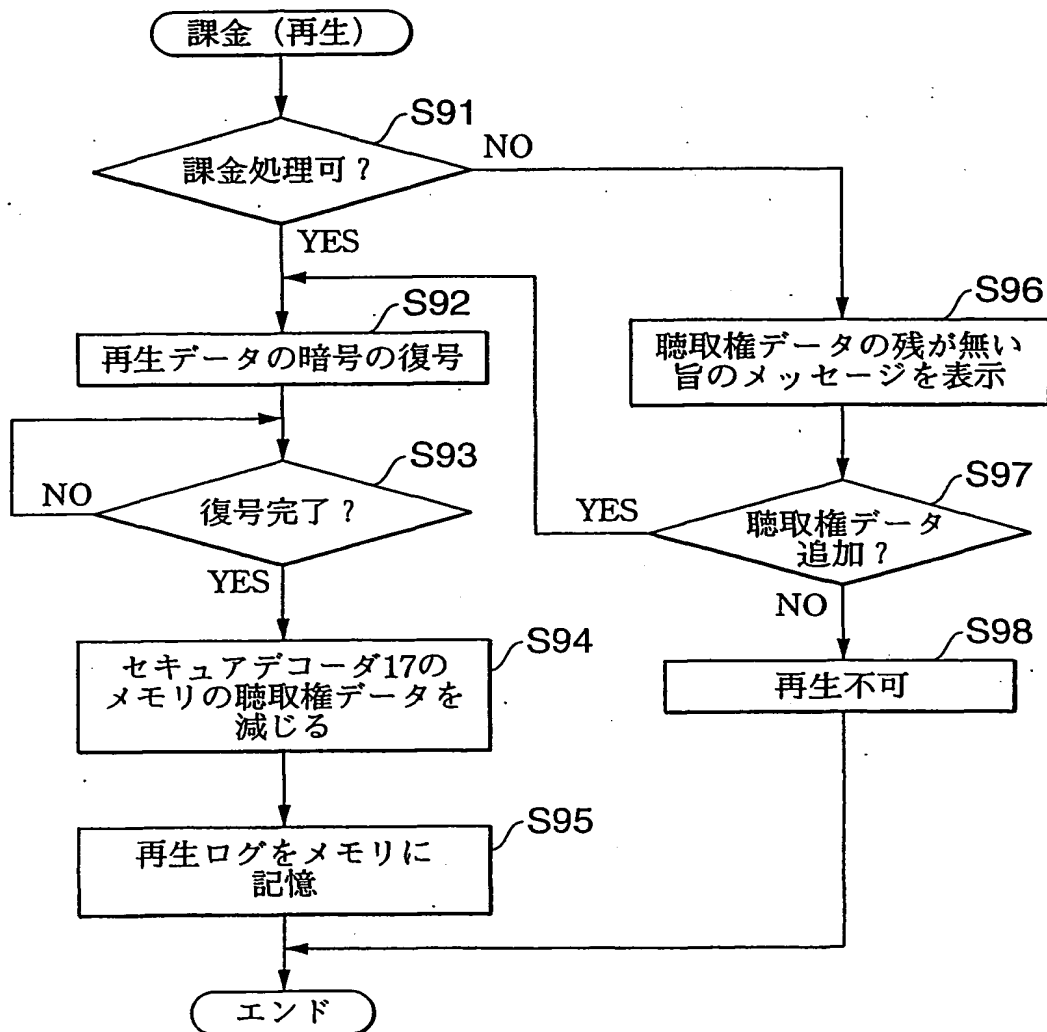


FIG.13

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP01/06183

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl⁷ G11B 20/10, G10F 3/06, G06F 17/60, G10K 15/02

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁷ G11B 20/10, H04N 5/91, G10F 3/06, G06F 17/60, G10K 15/02

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2001
Kokai Jitsuyo Shinan Koho	1971-2001	Jitsuyo Shinan Toroku Koho	1996-2001

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 11-238306 A (Fujitsu Limited), 31 August, 1999 (31.08.99), Full text; Figs. 1 to 18 & EP 000930616 A2 & CN 001227948 A	1-75
Y	JP 10-208388 A (Victor Company of Japan, Limited), 07 August, 1998 (07.08.98), Full text; Figs. 1 to 7 & EP 000853315 A2 & US 006097814 A1	1-75
Y	JP 11-306672 A (Sony Corporation), 05 November, 1999 (05.11.99), Full text; Figs. 1 to 8 (Family: none)	1-75
Y	JP 2000-113587 A (Sony Corporation), 21 April, 2000 (21.04.00), Full text; Figs. 1 to 10 (Family: none)	1-75
A	JP 2000-195161 A (Victor Company of Japan, Limited), 14 July, 2000 (14.07.00), Full text; Figs. 1 to 11 (Family: none)	1-75

☒ Further documents are listed in the continuation of Box C.
 ☐ See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier document but published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search
03 October, 2001 (03.10.01)Date of mailing of the international search report
16 October, 2001 (16.10.01)Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP01/06183

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 11-213554 A (Toshiba Corporation), 06 August, 1999 (06.08.99), Full text; Figs. 1 to 22 & CN 001220460 A	7-8, 35-36, 50-51, 68-69
A	JP 2000-156036 A (Sony Corporation), 06 June, 2000 (06.06.00), Full text; Figs. 1 to 5 (Family: none)	20-25, 44-49
A	JP 11-313282 A (Sanyo Electric Co., Ltd.), 09 November, 1999 (09.11.99), Full text; Figs. 1 to 16 & EP 000954173 A1	60-62, 70-72

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl⁷ G11B 20/10 G10F 3/06 G06F 17/60
G10K 15/02

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl⁷ G11B 20/10 H04N 5/91 G10F 3/06
G06F 17/60 G10K 15/02

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922-1996年
日本国公開実用新案公報 1971-2001年
日本国登録実用新案公報 1994-2001年
日本国実用新案登録公報 1996-2001年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	J P 11-238306 A (富士通株式会社) 31. 8月. 1999 (31. 08. 99) 全文 第1-18図 & E P 000930616 A2 & C N 001227948 A	1-75
Y	J P 10-208388 A (日本ビクター株式会社) 7. 8月. 1998 (07. 08. 98) 全文 第1-7図 & E P 000853315 A2 & U S 006097814 A1	1-75

☒ C欄の続きにも文献が列举されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的な技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日

03.10.01

国際調査報告の発送日

16.10.01

国際調査機関の名称及びあて先

日本国特許庁 (ISA/J P)
郵便番号100-8915
東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

宮下 誠

5Q

2946

電話番号 03-3581-1101. 内線 3589

C (続き) 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	J P 11-306672 A (ソニー株式会社) 5. 11月. 1999 (05. 11. 99) 全文 第1-8図 (ファミリーなし)	1-75
Y	J P 2000-113587 A (ソニー株式会社) 21. 4月. 2000 (21. 04. 00) 全文 第1-10図 (ファミリーなし)	1-75
A	J P 2000-195161 A (日本ビクター株式会社) 14. 7月. 2000 (14. 07. 00) 全文 第1-11図 (ファミリーなし)	1-75
A	J P 11-213554 A (株式会社東芝) 6. 8月. 1999 (06. 08. 99) 全文 第1-22図 & C N 001220460 A	7-8、35-36、 50-51、68-69
A	J P 2000-156036 A (ソニー株式会社) 6. 6月. 2000 (06. 06. 00) 全文 第1-5図 (ファミリーなし)	20-25、44-49
A	J P 11-313282 A (三洋電機株式会社) 9. 11月. 1999 (09. 11. 99) 全文 第1-16図 & E P 000954173 A 1	60-62、70-72

THIS PAGE BLANK (USPTO,